Citrix Access Gateway Standard Edition Administratordokumentation

Citrix Access Gateway™ 4.6, Standard Edition

Model 2000 Serie

Hinweise zu Copyright und Marken

Die Verwendung des in diesem Handbuch beschriebenen Produkts unterliegt der Annahme der Endbenutzerlizenzvereinbarung. Eine druckbare Kopie der Endbenutzerlizenzvereinbarung finden Sie auf den Installationsmedien.

Die in diesen Unterlagen enthaltenen Angaben und Daten können ohne vorherige Ankündigung geändert werden. Die in den Beispielen verwendeten Firmen, sonstigen Namen und Daten sind frei erfunden, sofern nichts anderes angegeben ist. Ohne ausdrückliche schriftliche Erlaubnis von Citrix Systems, Inc. darf kein Teil dieser Unterlagen für irgendwelche Zwecke vervielfältigt oder übertragen werden, unabhängig davon, auf welche Art und Weise oder mit welchen Mitteln, weder elektronisch noch mechanisch.

© 2003-2009 Citrix Systems, Inc. Alle Rechte vorbehalten.

Citrix und ICA (Independent Computing Architecture) sind eingetragene Marken und Access Gateway ist eine Markevon Citrix Systems, Inc. in den USA und anderen Ländern.

RSA Encryption © 1996-1997 RSA Security Inc. Alle Rechte vorbehalten.

Dieses Produkt enthält Software, die von Expat XML Parser entwickelt wurde © 1999 - 2009

Dieses Produkt enthält Software, die von Internet Systems Consortium entwickelt wurde © 2001 - 2009

Dieses Produkt enthält Software, die von Free Software Foundation, Inc. entwickelt wurde © 2007

Dieses Produkt enthält Software, die von Independent JPEG Group entwickelt wurde © 1991 - 1998

Dieses Produkt enthält Software, die von libpng.org entwickelt wurde © 1995 - 2009

Dieses Produkt enthält Software, die von OpenLDAP Foundation entwickelt wurde © 1998 - 2008

Dieses Produkt enthält Software, die von OpenSSL Project entwickelt wurde © 1998 - 2008

Dieses Produkt enthält zlib-Software, die von Jean-loup Gailly und Mark Adler entwickelt wurde © 1995 - 2005

Dieses Produkt enthält Software, die von SilverStripe Limited entwickelt wurde © 2006 - 2009

Lizenzierung: Teile dieser Dokumentation über Globetrotter, Macrovision und FLEXlm sind urheberrechtlich geschützt von © 2003-2006 Macrovision Corporation. Alle Rechte vorbehalten.

Apache Software Foundation

Copyright © 2009 Citrix Systems, Inc.

Lizenziert unter der Apache-Lizenz, Version 2.0 (die "Lizenz"); Sie dürfen diese Datei nur in Übereinstimmung mit der Lizenz verwenden. Sie erhalten eine Kopie der Lizenz an dieser Stelle:

http://www.apache.org/licenses/LICENSE-2.0

Außer wenn es durch das geltende Gesetz erforderlich ist oder schriftlich vereinbart wurde, wird die Software unter der Lizenz OHNE JEGLICHE HAFTUNG ODER KONDITIONEN bereitgestellt, weder ausdrücklich noch impliziert. Details über die geltenen Erlaubnisse und Einschränkungen finden Sie im Text der Lizenz.

Anerkennung von Marken

Adobe, Acrobat und PostScript sind Marken oder eingetragene Marken von Adobe Systems Incorporated in den USA und/oder anderen Ländern.

Java, Sun und SunOS sind Marken oder eingetragene Marken von Sun Microsystems, Inc. in den USA und anderen Ländern. Solaris ist eine eingetragene Marke von Sun Microsystems, Inc., die dieses Produkt nicht getestet oder anerkannt haben.

Teile dieser Software basieren partiell auf der Arbeit der Independent JPEG Group.

Teile dieser Software enthalten Imagingcode, der Eigentum und Copyright von Pegasus Imaging Corporation, Tampa, FL ist. Alle Rechte vorbehalten.

Macromedia und Flash sind Marken oder eingetragene Marken von Macromedia, Inc. in den USA und/oder anderen Ländern.

Microsoft, MS-DOS, Windows, Windows Media, Windows Server, Windows NT, Win32, Outlook, ActiveX, Active Directory und DirectShow sind eingetragene Marken oder Marken von Microsoft Corporation in den USA und/oder anderen Ländern.

Netscape und Netscape Navigator sind eingetragene Marken von Netscape Communications Corp. in den USA und anderen Ländern.

Lizenzierung: Globetrotter, Macrovision und FLEXlm sind Marken und/oder eingetragene Marken der Macrovision Corporation.

Alle anderen Marken und eingetragenen Marken sind das Eigentum ihrer jeweiligen Inhaber.

Dokumentcode: 1. Mai 2009 (bp)

Inhalt

Kapitel 1 Einführung

Hinweise zur Benutzung dieses Handbuchs 11
Typografische Konventionen 11
Service und technischer Support 12
Subscription Advantage 13
Knowledge Center-Benachrichtigungen 13
Schulung und Zertifizierung 13
Terminologieänderungen 14

Kapitel 2 Einführung in das Citrix Access Gateway

Access Gateway-Technologien 15
Access Gateway-Betriebsmodi 16
Funktionen des Access Gateways 17
Neue Features in diesem Release 18
Änderungen an Access Gateway-Features 19

Kapitel 3 Planen der Bereitstellung

Bereitstellen des Access Gateways 22
Access Gateway in der DMZ des Netzwerks 22
Installieren des Access Gateways in der DMZ 23
Access Gateway-Konnektivität in der DMZ 23
Access Gateway in einem gesicherten Netzwerk 24
Access Gateway-Konnektivität in einem gesicherten Netzwerk 24
Planen für Sicherheit im Access Gateway 25
Konfigurieren der sicheren Zertifikatverwaltung 25
Unterstützung bei der Authentifizierung 26

Bereitstellen des Access Gateways mit Citrix XenApp oder Citrix XenDesktop . 27
Bereitstellen von Access Gateway in einer Double-Hop-DMZ 27
Bereitstellen weiterer Geräte für Lastausgleich und Failover. 28
Bereitstellen von Access Gateway-Geräten hinter einem Load Balancer. 29
Bereitstellen von Access Gateway Advanced Edition 30
Konfigurieren mehrerer Server in einer Access-Serverfarm. 31

Kapitel 4 Erstmalige Installation des Access Gateways

Vorbereitung für die Installation von Access Gateway 33
Zubehör und erforderliche Informationen für die Installation. 34
Einrichten der Access Gateway-Hardware 35
Konfigurieren der TCP/IP-Einstellungen für Access Gateway 36
Konfigurieren der TCP/IP-Einstellungen mit der seriellen Konsole. 36
Konfigurieren der TCP/IP-Einstellungen mit Netzwerkkabeln. 38
Konfigurieren der TCP/IP-Einstellungen für eine Double-Hop-Bereitstellung 41
Neustarten des Access Gateways 42

Kapitel 5 Konfigurieren des Access Gateways für die Netzwerkumgebung

Installieren von Lizenzen. 43
Lizenztypen für Access Gateway. 44
Ermitteln von Lizenzierungsstatistiken 45
Abrufen Ihrer Lizenzdateien. 46
Konfigurieren von Lizenzen für mehrere Geräte. 48
Herunterladen von Lizenzprotokollen 49
Aktualisieren von Lizenzierungsinformationen. 49
Aktualisieren vorhandener Lizenzen 49
Kulanzzeitraum für die Lizenzierung. 50
Testen der Lizenzinstallation 50
Erstellen und Installieren von Zertifikaten 51
Übersicht über Zertifikatsignieranforderungen 52
Installieren eines Zertifikats und eines privaten Schlüssels von einem Windows-Computer aus 55
Installieren von Stammzertifikaten auf dem Access Gateway 56
Installieren mehrerer Stammzertifikate 57
Konfigurieren weiterer Netzwerkeinstellungen 58
Konfigurieren von Namensdienstanbietern 58
Bearbeiten der HOSTS-Datei. 59
Konfigurieren von dynamischen und statischen Routen 60

Konfigurieren von Datum und Uhrzeit auf dem Access Gateway 66
Konfigurieren eines NTP-Servers 66
Verwenden der Standardportalseite 67
Konfigurieren des Netzwerkzugriffs 69

Kapitel 6 Konfigurieren der Authentifizierung und Autorisierung

Voraussetzungen für die Authentifizierung auf dem Access Gateway 72
Konfigurieren der Authentifizierung auf dem Access Gateway 72
Konfigurieren des Bereichs "Default" 75
Erstellen von zusätzlichen Bereichen 76
Konfigurieren der lokalen Authentifizierung 78
Konfigurieren lokaler Benutzer 79
Zuweisen von Benutzern zu mehreren Gruppen 80
Ändern von Kennwörtern für Benutzer 81
Konfigurieren von LDAP-Authentifizierung und -Autorisierung 81
Konfigurieren der LDAP-Autorisierung 86
Gruppenattributfelder für die LDAP-Autorisierung 87
Verwenden von Zertifikaten für sichere LDAP-Verbindungen 89
Bestimmen der Attribute in Ihrem LDAP-Verzeichnis 89
Konfigurieren von RADIUS-Authentifizierung und -Autorisierung 90
RADIUS-Autorisierung 93
Auswählen der RADIUS-Authentifizierungsprotokolle 94
Konfigurieren der RSA SecurID-Authentifizierung 95
Konfigurieren der RSA-Einstellungen für einen Cluster 98
Zurücksetzen des Node Secrets 98
Konfigurieren der Authentifizierung mit Secure Computing SafeWord 99
Konfigurieren der SafeWord-Einstellungen auf dem Access Gateway 100
Konfigurieren der Autorisierung mit SafeWord 101
Konfigurieren der Gemalto Protiva-Authentifizierung 102
Konfigurieren der Gemalto Protiva-Einstellungen 102
Konfigurieren von NTLM-Authentifizierung und -Autorisierung 103
Konfigurieren der NTLM-Autorisierung 105
Konfigurieren von erweiterten Optionen für die Authentifizierung 106
Konfigurieren des Benutzernamenpräfixes 106
Konfigurieren der Authentifizierung für die Verwendung von Einmal-Kennwörtern 107
Verbergen der Aufforderung für die Antwortüberprüfung 108
Konfigurieren von Zweimethodenauthentifizierung 108
Ändern der Beschriftung von Kennwortfeldern 110

Kapitel 7 Konfigurieren von Netzwerkzugriff und Gruppenressourcen

Konfigurieren des Netzwerkrouting 112
Bereitstellen von Netzwerkzugriff für Benutzer 112
Aktivieren von Split-Tunneling und zugänglichen Netzwerken 114
Konfigurieren von Benutzergruppen 115
Konfigurieren von Zugriffssteuerungslisten 116
Erstellen lokaler Benutzergruppen 116
Konfigurieren von Ressourcengruppen 117
Erstellen von Benutzergruppen 118
Eigenschaften der Standardgruppe ("Default") 119
Konfigurieren von Ressourcen für eine Benutzergruppe 120
Konfigurieren von Benutzern, die mehreren Gruppen angehören 121
Konfigurieren von Netzwerkressourcen 122
Zulassen und Verweigern von Netzwerkressourcen und Anwendungsrichtlinien 125
Festlegen von Anwendungsrichtlinien 126
Konfigurieren von Endpunktrichtlinien und -ressourcen 129
Erstellen einer Endpunktrichtlinie für eine Gruppe 130
Festlegen der Priorität von Gruppen 134
Konfigurieren von Vorauthentifizierungsrichtlinien 135
Konfigurieren des Access Gateways für Citrix Branch Repeater 136

Kapitel 8 Konfigurieren von Benutzerverbindungen für das Citrix Access Gateway Plug-in

Systemvoraussetzungen 138
Betriebssysteme 138
Webbrowser 138
Funktionsweise von Benutzerverbindungen 139
Einrichten des sicheren Tunnels 140
Tunneln des privaten Netzwerkverkehrs über sichere Verbindungen 140
Beenden des sicheren Tunnels und Zurücksenden von Paketen an den Client . . . 142
Unterstützen des Access Gateway Plug-ins 143
Konfigurieren von Proxyservern für das Access Gateway Plug-in 144
Installieren des Access Gateway Plug-ins mit dem MSI-Paket 145
Installation des MSI-Pakets mit einer Gruppenrichtlinie 146
Installieren des MSI-Pakets durch Ankündigen 146
Konfigurieren von Single Sign-on für Windows-Betriebssysteme 148
Verbinden mit früheren Versionen des Access Gateway Plug-ins 149
Aktualisieren von früheren Versionen des Access Gateway Plug-ins 149

Herstellen einer Verbindung mit einer Webadresse 150
Anmelden mit dem Access Gateway Plug-in 152
Installieren des Access Gateway Plug-ins für Linux. 156
Konfigurieren der Authentizierungsanforderungen nach einer Netzwerkunterbrechung 158
Konfigurieren weiterer Gruppeneigenschaften 159
Aktivieren von IP-Pooling 159
Split DNS aktivieren. 161
Aktivieren von internem Failover 161
Aktivieren von Domänenanmeldeskripten. 162
Aktivieren von Sitzungstimeouts für Access Gateway Plug-ins 163
Konfigurieren von Websitzungstimeouts. 164
Anfordern von Clientzertifikaten für die Authentifizierung 165
Definieren von Clientzertifikatskriterien 165
Verwenden von Clientzertifikaten mit Access Gateway Advanced Edition. . 167
Installieren von Stammzertifikaten 167
Abrufen eines Stammzertifikats von einer Zertifizierungsstelle 168
Installieren von Stammzertifikaten auf einem Clientgerät 168
Auswählen einer Verschlüsselungsart für Clientverbindungen 169

Kapitel 9 Konfigurieren von Anmelde- und Portalseiten für das Citrix Access Gateway Plug-in

Konfigurieren der Access Gateway-Anmeldeseiten 172
Aktivieren der Anmeldeseitenauthentifizierung 172
Anpassen der Anmeldeseite 172
Access Gateway-Portalseitenvorlagen. 174
Herunterladen von und Arbeiten mit Portalseitenvorlagen 174
Installieren benutzerdefinierter Portalseitendateien. 176
Auswählen einer Portalseite für eine Gruppe. 177
Konfigurieren einer Portalseite mit mehreren Anmeldeoptionen. 178
Anmelden, wenn Vorauthentifizierungsrichtlinien konfiguriert sind. 179

Kapitel 10 Wartung des Access Gateways

Access Gateway-Verwaltungstools 181
Administration Tool 182
Administration Portal 184
Aktualisieren der Access Gateway-Software 186
Installieren des Software-Upgrades 188

Neuinstallieren der Access Gateway-Software 189
Neuinstallation der Software bei Model 2000 190
Neuinstallation der Software bei Model 2010 190
Speichern und Wiederherstellen der Access Gateway-Konfiguration 192
Neustarten und Herunterfahren des Access Gateways 194
Neustarten des Access Gateways 194
Herunterfahren des Access Gateways 195
Initialisieren des Access Gateways 195
Zulassen von ICMP-Verkehr 196
Konfigurieren persönlicher Firewalls von Drittanbietern 196
McAfee Personal Firewall Plus 198
Norton Personal Firewall 198
Sygate Personal Firewall (kostenlose und Pro-Version) 198
Tiny Personal Firewall 199
ZoneAlarm Pro 199

Kapitel 11 Installieren zusätzlicher Access Gateway-Geräte

Erstellen eines Clusters mit Access Gateway-Geräten 203
Konfigurieren mehrerer Geräte für die Verwendung eines Load Balancers 206
Konfigurieren des Lastausgleichs 207
Konfigurieren von Access Gateway-Geräten für den Betrieb hinter einem Load Balancer 208
Konfigurieren des Load Balancing mit Advanced Access Control. 211
Konfigurieren von Access Gateway-Failover 212

Anhang A Überwachen des Access Gateways

Anzeigen und Herunterladen von Systemmeldungsprotokollen. 216
Anzeigen der Access Gateway Plug-in-Verbindungsprotokolle 217
Weiterleiten von Systemmeldungen an einen Syslogserver 218
SNMP-Protokolle. 219
Beispiel für eine MRTG-Ausgabe 219
Anzeigen von Systemstatistiken 221
Überwachen der Access Gateway-Operationen 221

Anhang B Sichern von Verbindungen mit digitalen Zertifikaten

Einführung in Sicherheitsprotokolle, Kryptografie und digitale Zertifikate 224
Einführung in Sicherheitsprotokolle 224
Einführung in die Kryptografie 225
Digitale Zertifikate und Zertifizierungsstellen. 227

Beantragen von Zertifikaten. 231
Ihre Organisation hat eine eigene Zertifizierungsstelle 232
Ihre Organisation hat keine eigene Zertifizierungsstelle 232
Beantragen von Serverzertifikaten. 233
Digitale Zertifikate und deren Verwendung im Access Gateway 233
Verwenden von Windows-Zertifikaten 234
Entschlüsseln des privaten Schlüssels 235
Umwandeln in ein PEM-formatiertes Zertifikat 235
Kombinieren des privaten Schlüssels mit dem signierten Zertifikat. 237
Generieren vertrauenswürdiger Zertifikate für mehrere Ebenen. 238
Anfordern von Zertifikaten für interne Verbindungen 239
Verwenden von Platzhalterzertifikaten 240

Anhang C Beispiele für die Konfiguration des Netzwerkzugriffs

Konfigurationsbeispiele 243
Konfigurieren der LDAP-Authentifizierung und -Autorisierung. 244
Vorbereiten der Konfiguration von LDAP-Authentifizierung und -Autorisierung 245
Konfigurieren des Access Gateways zur Unterstützung des Zugriffs auf die internen Netzwerkressourcen 250
Szenario für das Erstellen von Gastkonten mit der Liste "Local Users" 262
Erstellen eines Authentifizierungsbereichs für Gastbenutzer 263
Erstellen lokaler Benutzer. 264
Erstellen und Zuweisen einer Netzwerkressource für die Standardbenutzergruppe 265
Szenario für das Konfigurieren der lokalen Autorisierung für lokale Benutzer. . 266

Anhang D Problembehandlung beim Access Gateway

Problembehandlung bei Webinterface-Verbindungen 269
Das Webinterface wird angezeigt, ohne dass Anmeldeinformationen eingegeben wurden. 269
Nach dem Anmelden werden keine Anwendungen angezeigt 270
Benutzer werden zu einer Anmeldeseite geleitet, auf der sie zum Starten des Access Gateway Plug-ins aufgefordert werden 271

Sonstige Probleme 271
Lizenzdatei stimmt nicht mit dem Access Gateway überein. 271
Definieren von Subnetzeinschränkungen für zugängliche Netzwerke 272
Virtualisierungssoftware. 272
ICMP-Übertragungen 272
Ping-Befehl 272
LDAP-Authentifizierung 272
Endpoint Policies (Endpunktrichtlinien) 273
Netwerkressourcen 273
Internes Failover 273
Zertifikatsignierung 274
Zertifikatsperrlisten. 274
Netzwerkmeldungen an nicht vorhandene IP-Adressen 274
Das Access Gateway startet nicht und die serielle Konsole ist leer 275
Zugriff auf das Administration Tool nicht möglich. 275
Kommunikation zwischen Geräten und dem Access Gateway nicht möglich 275
Verwenden von Strg+Alt+Entf zum Neustarten des Access Gateways nicht möglich 275
Sitzungen mit SSL Version 2 und Zertifikatketten auf mehreren Ebenen . . . 276
H.323-Protokoll 276
Zertifikate mit 512-Bit-Schlüsselpaaren 276
Laufwerkszuordnung kann nicht mit einer Anwendungsrichtlinie eingeschränkt werden. 276
Citrix Access Gateway Plug-in 277
Access Gateway Plug-in-Verbindungen mit Windows XP. 277
DNS-Namensauflösung mit Namensdienstanbietern 277
Funktion zum automatischen Aktualisieren. 277
Von Windows Server 2003-Computern ausgehende Clientverbindungen . . . 277
NTLM-Authentifizierung. 277
WINS-Einträge 278
Verwendung von Drittanbieter-Clientsoftware 278

Einführung

Hinweise zur Benutzung dieses Handbuchs

Dieses Benutzerhandbuch richtet sich an Systemadministratoren, die mit der Installation und Konfiguration des Access Gateways betraut wurden. Dabei wird davon ausgegangen, dass das Access Gateway mit einem vorhandenen Netzwerk verbunden ist und dass der Administrator über die notwendigen Kenntnisse zum Konfigurieren dieses Netzwerks verfügt.

Bei den Konfigurationsschritten in diesem Dokument wird vorausgesetzt, dass das Access Gateway als eigenständige Anwendung bereitgestellt wird und dass Benutzer eine direkte Verbindung zum Access Gateway herstellen.

Dieses Benutzerhandbuch enthält auch Informationen, wie Sie das Access Gateway für die Zusammenarbeit mit Access Gateway Advanced Edition konfigurieren. Weitere Informationen hierzu finden Sie unter "Bereitstellen von Access Gateway Advanced Edition" auf Seite 30.

Typografische Konventionen

In der Access Gateway-Dokumentation werden die folgenden typografischen Konventionen für Menüs, Befehle, Tasten und Objekte in der Benutzeroberfläche des Programms verwendet:

Konvention	Bedeutung
Fettdruck	Befehle, Namen von Benutzeroberflächenobjekten, z.B. Textfelder und Optionsschaltflächen, sowie Benutzereingaben.
Kursiv	Platzhalter für Informationen oder Parameter, die Sie eingeben müssen. *Dateiname* in einem Verfahren bedeutet z.B., dass Sie den tatsächlichen Namen einer Datei eingeben müssen. Außerdem werden neue Begriffe sowie die Titel von Dokumentationen in Kursivschrift angegeben.
%SystemRoot%	Das Windows-Systemverzeichnis, das WTSRV, WINNT, WINDOWS oder ein anderer Verzeichnisname sein kann, den Sie bei der Installation von Windows angegeben haben.

Konvention	Bedeutung
`Nichtproportional`	Text, der in einer Textdatei angezeigt wird.
{geschweifte Klammern}	Eine Reihe von Elementen, von denen eines in Befehlsanweisungen erforderlich ist. Beispiel: **{ Ja | Nein }** bedeutet, dass Sie **Ja** oder **Nein** eingeben müssen. Die geschweiften Klammern selbst müssen nicht eingegeben werden.
[eckige Klammern]	Optionale Elemente in Befehlsanweisungen. Zum Beispiel bedeutet [**/ping**], dass Sie **/ping** zusammen mit dem Befehl eingeben können. Geben Sie die eckigen Klammern selbst nicht mit ein.
| (vertikaler Strich)	Ein Trennzeichen zwischen Elementen in geschweiften oder eckigen Klammern in Befehlsanweisungen. Beispiel: **{ /hold | / release | /delete }** bedeutet, dass Sie **/hold** oder /release oder **/delete** eingeben.
… (Auslassung)	Sie können das vorherige Element bzw. die vorherigen Elemente in Befehlsanweisungen wiederholen. Zum Beispiel bedeutet **/ route:***Gerätename*[,…], dass Sie zusätzliche *Gerätenamen* eingeben können, die durch Kommas getrennt werden.

Service und technischer Support

Citrix bietet technischen Support hauptsächlich durch das CSN-Netzwerk (Citrix Solutions Network) an. Unsere CSN-Partner verfügen über entsprechendes Training und bieten unseren Kunden ein hohes Niveau an Support. Wenden Sie sich zuerst an Ihren Vertragshändler oder suchen Sie unter http://support.citrix.com nach dem nächstgelegenen CSN-Partner.

Zusätzlich zum CSN-Programm bietet Citrix im Knowledge Center eine Reihe von webbasierten Selbstbedienungstools für den technischen Support.Das Knowledge Center finden Sie unter http://support.citrix.com/. Es bietet Folgendes:

- Eine Knowledge Base mit technischen Lösungen zur Unterstützung der Citrix Umgebung
- Eine Onlinebibliothek der Produktdokumentation
- Interaktive Support-Foren für jedes Citrix Produkt
- Zugang zu den neuesten Hotfixes und Service Packs
- Security Bulletins
- Onlineproblemmeldung und -verfolgung (für Organisationen mit gültigen Supportverträgen)

Eine andere Supportquelle, Citrix Preferred Support Services, bietet eine Reihe von Optionen, sodass Sie den Grad und die Art von Support für die Citrix Produkte in Ihrer Organisation anpassen können.

Subscription Advantage

Ihr Produkt schließt das Abonnement Subscription Advantage für ein Jahr ein. Citrix Subscription Advantage bietet eine einfache Möglichkeit, stets aktuelle Softwareversionen und Informationen für Ihre Citrix Produkte zu haben. Abonnenten erhalten nicht nur automatisch Zugriff auf den Download der neuesten Feature Releases, Softwareupgrades und Erweiterungen, die während der Laufzeit des Abonnements verfügbar werden, sondern haben auch bevorzugten Zugang zu wichtigen technischen Informationen von Citrix.

Weitere Informationen finden Sie auf der Website von Citrix unter http://www.citrix.com. Klicken Sie auf der Homepage auf **Support > Subscription Advantage**.

Weitere Informationen erhalten Sie auch von Ihrem Vertragshändler, Citrix Customer Care oder einem Mitglied des Citrix Solutions Advisors-Programms.

Knowledge Center-Benachrichtigungen

Im Citrix Knowledge Center können Sie Benachrichtigungen konfigurieren, sodass Sie eine Nachricht erhalten, wenn ein Bereich aktualisiert wird, der Sie interessiert. Sie können Benachrichtigungen für Produktkategorien einstellen. Wenn es ein Update für das Produkt gibt, erhalten Sie eine Nachricht.

Melden Sie sich dafür bei der Citrix Support-Website unter http://support.citrix.com/ an. Wählen Sie nach dem Anmelden unter **Products**, ein Produkt aus. Klicken Sie unter **Alerts** auf **Add to your Alerts**. Um die Benachrichtigung anzuhalten, klicken Sie für das Product im Knowledge Center auf **Remove from your Alerts**.

Schulung und Zertifizierung

Citrix bietet eine Reihe von unterrichteten (ILT, engl. instructor led training) und webbasierten Kursen (WBT, engl.web-based training). Die von einem Schulungsleiter durchgeführten ILT-Kurse werden von Citrix Authorized Learning Centers (CALCs) angeboten. CALCs bieten hochwertige Schulungen mit den professionellen Schulungsmaterialien von Citrix. Viele dieser Kurse bereiten auf eine Zertifizierung vor.

Webbasierte Schulungskurse werden von CALCs, Wiederverkäufern und über die Website von Citrix angeboten.

Informationen zu Programmen und Courseware für Citrix Schulungen und Zertifizierungen finden Sie unter http://www.citrixtraining.com/.

Terminologieänderungen

Es gibt einige Namensänderungen für die Clientsoftware und für Citrix Produktnamen. Im Folgenden wird die aktualisierte Terminologie aufgelistet, die in dieser Dokumentation verwendet wird.

Früher	**Jetzt**
Access Gateway mit Advanced Access Control	Access Gateway Advanced Edition
Access Suite Console	Access Management Console
Secure Access Client	Access Gateway Plug-in
Citrix Presentation Server	Citrix XenApp
Citrix Presentation Server Clients	Citrix XenApp Plug-ins
Citrix Presentation Server Console	Citrix Erweiterte XenApp-Konfiguration
Webclient	Citrix XenApp Web Plug-in
Program Neighborhood Agent	Citrix XenApp (Plug-in)
Citrix WANScaler	Citrix Branch Repeater
WANScaler Client	Repeater Plug-in

Literaturhinweise

Weitere Informationen zu Access Gateway finden Sie in den folgenden Dokumenten:

- Installationsübersicht für Citrix Access Gateway Standard Edition
- Citrix Access Gateway Standard Edition Pre-Installation Checklist
- Citrix Access Gateway Standard Edition Integration Guide with Citrix XenApp and Citrix XenDesktop
- Citrix Access Gateway Standard Edition – Readme

Einführung in das Citrix Access Gateway

Citrix Access Gateway ist eine sichere Anwendungszugriffslösung, die Administratoren durch Richtlinien auf Anwendungsebene und Aktionssteuerung ermöglicht, den Zugriff auf Anwendungen und Daten zu sichern während sie Benutzern gleichzeitig ermöglichen, an einem beliebigen Ort zu arbeiten. IT-Administratoren erhalten eine Steuerungszentrale und Tools, die sie dabei unterstützen, Regelungen einzuhalten und hochgradige Informationssicherheit innerhalb und außerhalb des Unternehmens zu gewährleisten. Gleichzeitig gibt es Benutzern einen einzelnen Zugriffspunkt zu den Unternehmensanwendungen und Daten, die sie benötigen – optimiert anhand von Rollen, Geräten und Netzwerken. Diese einzigartige Kombination von Funktionen hilft, die Produktivität der heutigen, mobilen Mitarbeiter zu maximieren.

Dieses Kapitel enthält:

- "Access Gateway-Technologien"
- "Access Gateway-Betriebsmodi"

Access Gateway-Technologien

Das Access Gateway lässt sich schnell und einfach bereitstellen und verwalten. Das Access Gateway wird dabei in den meisten Fällen hinter der Firewall oder in der DMZ platziert. Es werden aber auch komplexere Bereitstellungen unterstützt, z. B. bei Verwendung eines Server Load Balancers oder einer Double-Hop-DMZ.

Wenn das Access Gateway zum ersten Mal gestartet wird, müssen Sie mit dem Access Gateway Administration Tool die für das interne Netzwerk geltenden Grundeinstellungen konfigurieren. Dazu gehören die IP-Adresse, die Subnetzmaske, die IP-Adresse des Standardgateways und die DNS-Adresse. Sobald die Grundeinstellungen konfiguriert wurden und eine Verbindung mit dem Netzwerk hergestellt wurde, können Sie die Einstellungen konfigurieren, die für den Einsatz dieses konkreten Access Gateway-Geräts gelten sollen. Dazu gehören die Optionen für die Authentifizierung, die Autorisierung und die gruppenbasierte Zugriffssteuerung, die Endpunktressourcen und -richtlinien, die Portalseiten sowie die IP-Pools.

Weitere Informationen zum Installieren des Access Gateways finden Sie in der *Installationsübersicht für Citrix Access Gateway Standard Edition* oder unter "Erstmalige Installation des Access Gateways" auf Seite 33.

Access Gateway-Betriebsmodi

Das Access Gateway kann auf verschiedene Arten verwendet werden:

- **Verbindungen nur über das Gerät:** In diesem Szenario wird das Access Gateway als eigenständiges Gerät in der DMZ installiert. Benutzer stellen mit dem Citrix Access Gateway Plug-in direkt eine Verbindung zum Access Gateway her und erhalten so Zugriff auf Netzwerkressourcen, z. B. E-Mail- und Webserver.
- **Verbindungen über das Webinterface, Citrix XenApp oder Citrix XenDesktop:** In diesem Szenario melden sich Benutzer am Webinterface an und werden dann mit den veröffentlichten Anwendungen in XenApp oder den veröffentlichten Desktops in XenDesktop verbunden. Abhängig davon, wie das Access Gateway mit XenApp bereitgestellt wird, können Benutzer sich nur mit den Citrix XenApp Plug-ins (der neue Name für Citrix Presentation Server Clients), nur mit dem Access Gateway Plug-in oder gleichzeitig mit beiden Plug-ins verbinden. Benutzer verbinden sich mit veröffentlichten Desktops über Citrix Desktop Receiver. Weitere Informationen finden Sie in der *Citrix Access Gateway Standard Edition – Integrationsdokumentation für Citrix XenApp und Citrix XenDesktop*.

Hinweis: Die Installation von Desktop Receiver oder Desktop Receiver Embedded Edition auf dem gleichen Computer wie die XenApp Plug-ins (die Clientsoftware für Citrix XenApp) wird nicht unterstützt. Wenn Benutzer vom gleichen Computer sowohl auf virtuelle Desktops als auch auf virtuelle Anwendungen zugreifen sollen, empfiehlt Citrix, die XenApp Plug-ins auf den virtuellen Desktops zu installieren, die Sie mit XenDesktop erstellen. So können auf den virtuellen Desktops virtuelle Anwendungen verwendet werden.

- **Verbindungen mit Access Gateway Advanced Edition:** In diesem Szenario ist das Access Gateway in der DMZ installiert. Anfängliche TCP/IP-Einstellungen für das Gerät werden während der Installation des Geräts konfiguriert. Erweiterte Einstellungen für die Verwaltung des Access Gateways werden mit der Access Management Console konfiguriert, die Teil von Access Gateway Advanced Edition ist. Weitere Informationen finden Sie unter "Bereitstellen von Access Gateway Advanced Edition" auf Seite 30 oder in der *Citrix Access Gateway Advanced Edition – Administratordokumentation*.

Funktionen des Access Gateways

Das Access Gateway übernimmt die folgenden Funktionen:

- Authentifizierung
- Terminierung verschlüsselter Sitzungen
- Zugriffssteuerung (auf der Basis von Berechtigungen)
- Weiterleitung des Datenverkehrs (wenn die ersten drei Funktionen erfüllt wurden)

Als eigenständiges Gerät in der DMZ arbeitet das Access Gateway folgendermaßen:

- Remotebenutzer laden das Access Gateway Plug-in herunter, indem sie eine Verbindung zu einer sicheren Webadresse herstellen und ihre Authentifizierungsinformationen eingeben.
- Nach dem Download des Access Gateway Plug-ins melden sich die Benutzer an. Wenn die Authentifizierung erfolgreich war, richtet das Access Gateway einen sicheren Tunnel ein.

- Sobald Remotebenutzer versuchen, über den VPN-Tunnel auf die Netzwerkressourcen zuzugreifen, verschlüsselt das Access Gateway Plug-in den gesamten Netzwerkverkehr, der für das Intranet der Organisation bestimmt ist, und leitet die Pakete an das Access Gateway weiter.
- Das Access Gateway fungiert als Endpunkt des SSL-Tunnels (terminiert den Tunnel), akzeptiert den eingehenden Verkehr, der für das private Netzwerk bestimmt ist, und leitet den Verkehr an das private Netzwerk weiter. Das Access Gateway sendet den Verkehr über einen sicheren Tunnel zum Remotecomputer zurück.

Neue Features in diesem Release

Diese Version von Access Gateway Standard Edition enthält folgende neue Funktionen:

- **Neues Betriebssystem:** Das Betriebssystem auf dem Access Gateway wurde aktualisiert.

  Wichtig: Mit diesem Update wird eine Upgrade von früheren Versionen des Access Gateways nicht unterstützt. Sie müssen eine vollständige Neuinstallation von Version 4.6 auf dem Access Gateway-Gerät durchführen. Weitere Informationen hierzu finden Sie unter "Neuinstallieren der Access Gateway-Software" auf Seite 189.

- **Verbesserte Verwaltung des Access Gateways:** Administration Desktop ist in das Administration Tool integriert und ermöglicht so eine bequemere und schnellere Überwachung der Clientverbindungen.
- **Unterstützung für Citrix XenDesktop:** Sie können das Access Gateway für den Benutzerzugriff auf veröffentlichte Desktops konfigurieren. Sie konfigurieren das Access Gateway auf die gleiche Weise wie für Citrix XenApp und geben dabei die Webinterface-Informationen an, die Sie in XenDesktop konfiguriert haben. Weitere Informationen finden Sie in der *Citrix Access Gateway Standard Edition – Integrationsdokumentation für Citrix XenApp und Citrix XenDesktop*.
- Unterstützung für Gemalto Protiva-Authentifizierung: Sie können einen Authentifizierungsbereich (authentication realm) konfigurieren für die Unterstützung von Gemalto Protiva-Authentifizierung mit RADIUS-basierter Authentifizierung. Benutzer verwenden bei der Anmeldung einen Code, den sie von einem Gemalto-Token erhalten.

- Neues MSI-Paket für das Access Gateway Plug-in: Ermöglicht die zentrale Verwaltung und richtlinienbasierte Distribution des Access Gateway Plug-ins.
- Aktualisiertes Access Gateway Plug-in für Linux: Das Access Gateway Plug-in für Linux ermöglicht Verbindungen zum Access Gateway von allen unterstützten Linux-basierten Clientgeräten. Das Plug-in unterstützt Linux Kernel 2.6.x.
- **Unterstützung für XenDesktop-Verbindungslizenzen:** Sie können Lizenzdateien installieren, die nur Verbindungen zu Citrix XenDesktop zulassen. Wenn Benutzer eine Verbindung herstellen, können sie die Sitzung nur über den Citrix Desktop Receiver erstellen. Verbindungen mit dem Access Gateway Plug-in werden verhindert. XenDesktop-Verbindungslizenzen sind in den Editionen Citrix XenDesktop Standard, Advanced und Enterprise ab Juni 2009 enthalten. XenDesktop Platinum Edition enthält die universelle Access Gateway-Lizenz, die alle Access Gateway-Features aktiviert.
- **Rückwärtskompatibilität für das Administration Tool:** Wenn Sie das Administration Tool für Access Gateway Standard Edition Version 4.6 installieren und ältere Versionen des Geräts im Netzwerk installiert sind, können Sie mit Version 4.6 des Administration Tools Einstellungen auf älteren Versionen des Geräts konfigurieren.

Änderungen an Access Gateway-Features

Die folgenden Access Gateway-Features wurden aus dem Access Gateway entfernt:

- Kioskmodus
- Desktopfreigabe
- Administration Desktop und Real-Time Monitor

KAPITEL 3

Planen der Bereitstellung

In diesem Kapitel werden Bereitstellungsszenarios für das Access Gateway vorgestellt.

Sie können das Access Gateway am Rand des internen Netzwerks (Intranet) Ihres Unternehmens bereitstellen, sodass ein zentraler Zugriffspunkt auf alle Servern, Anwendungen und andere Netzwerkressourcen im internen Netzwerk entsteht. Alle Remotebenutzer müssen eine Verbindung zum Access Gateway herstellen, bevor sie auf die Ressourcen im internen Netzwerk zugreifen können.

In diesem Abschnitt wird auch die Bereitstellung des Access Gateways mit Citrix XenApp oder Citrix XenDesktop besprochen. Wenn Citrix XenApp Teil der Bereitstellung ist, können Sie das Access Gateway in einer Single-Hop- oder einer Double-Hop-DMZ-Konfiguration bereitstellen. Double-Hop-Bereitstellungen werden nicht für Citrix XenDesktop unterstützt. Weitere Informationen über die Bereitstellung des Access Gateways mit einer Serverfarm finden Sie in der *Citrix Access Gateway Standard Edition – Integrationsdokumentation für Citrix XenApp und Citrix XenDesktop*.

Dieses Kapitel enthält:

- "Bereitstellen des Access Gateways"
- "Access Gateway in der DMZ des Netzwerks"
- "Access Gateway in einem gesicherten Netzwerk"
- "Planen für Sicherheit im Access Gateway"
- "Bereitstellen des Access Gateways mit Citrix XenApp oder Citrix XenDesktop"
- "Bereitstellen von Access Gateway in einer Double-Hop-DMZ"
- "Bereitstellen weiterer Geräte für Lastausgleich und Failover"
- "Bereitstellen von Access Gateway Advanced Edition"

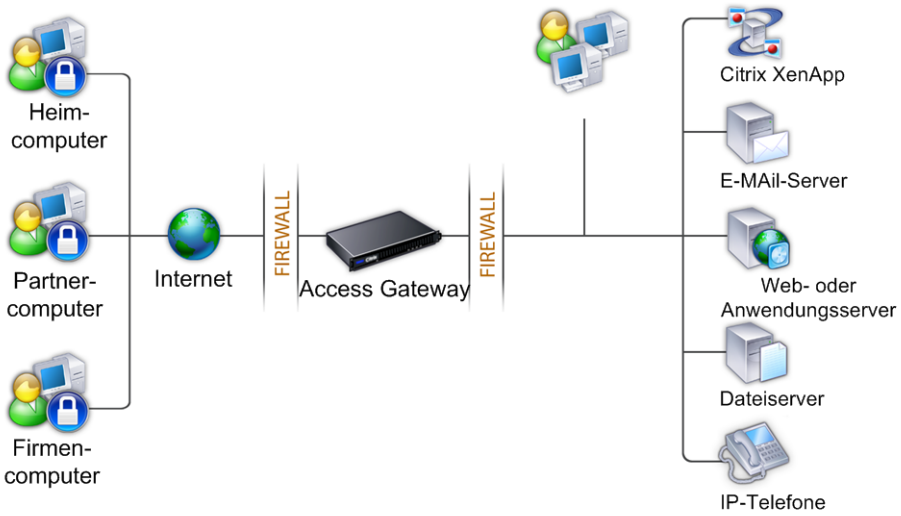
Bereitstellen des Access Gateways

In diesem Abschnitt werden die folgenden Access Gateway-Bereitstellungen erläutert:

- Bereitstellen des Access Gateways in der demilitarisierten Zone (DMZ) des Netzwerks
- Bereitstellen des Access Gateways in einem gesicherten Netzwerk, das keine DMZ besitzt
- Bereitstellen weiterer Access Gateway-Geräte für Lastausgleich und Failover

Access Gateway in der DMZ des Netzwerks

Viele Unternehmen schützen ihr internes Netzwerk mithilfe einer DMZ. Eine DMZ ist ein Subnetz, das zwischen dem sicheren internen Netzwerk des Unternehmens und dem Internet (oder einem externen Netzwerk) liegt. Wenn Access Gateway in der DMZ bereitgestellt wird, greifen Benutzer darauf mit dem Citrix Access Gateway Plug-in oder den Citrix XenApp Plug-ins zu (der neue Name für Citrix Presentation Server Clients).



Access Gateway in der DMZ

Installieren des Access Gateways in der DMZ

In dieser Konfiguration wird das Access Gateway in der DMZ installiert und so konfiguriert, dass eine Verbindung sowohl zum Internet als auch zum internen Netzwerk hergestellt wird. Zur Installation und Konfiguration folgen Sie den Anweisungen unter "Erstmalige Installation des Access Gateways" auf Seite 33.

Access Gateway-Konnektivität in der DMZ

Wenn Sie das Access Gateway in der DMZ bereitstellen, müssen die Clientverbindungen die Firewall überwinden, um eine Verbindung zum Access Gateway herstellen zu können. Standardmäßig erfolgt diese Verbindung mit SSL (Secure Sockets Layer) an Port 443. Damit diese Verbindung möglich ist, müssen Sie die Verwendung von SSL an Port 443 durch die erste Firewall zulassen.

Hinweis: Sie können den Port ändern, über den die Clientgeräte eine Verbindung zum Access Gateway aufbauen. Bearbeiten Sie hierzu die Porteinstellung im Administration Tool. Weitere Informationen zu dieser Porteinstellung finden Sie unter "Konfigurieren der TCP/IP-Einstellungen mit Netzwerkkabeln" auf Seite 38.

Das Access Gateway entschlüsselt die SSL-Verbindungen vom Gerät und baut stellvertretend für den Client eine Verbindung zu den Netzwerkressourcen hinter der zweiten Firewall auf. Die Ports, die für die Durchquerung der zweiten Firewall geöffnet sein müssen, sind abhängig von den Netzwerkressourcen, für deren Zugriff die externen Benutzer autorisiert sind.

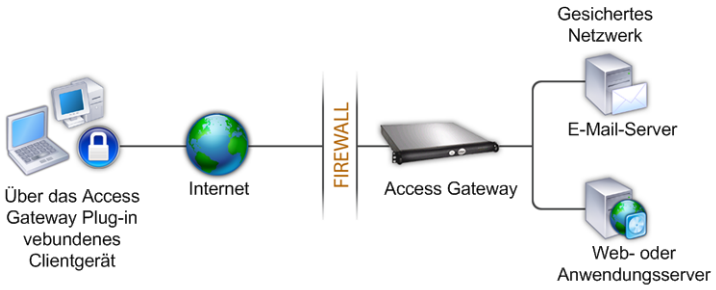
Wenn Sie beispielsweise die externen Benutzer für den Zugriff auf einen Webserver im internen Netzwerk autorisieren und der Server Port 80 nach HTTP-Verbindungen abhört, muss entsprechend HTTP an Port 80 durch die zweite Firewall zugelassen werden. Stellvertretend für die externen Clientgeräte stellt das Access Gateway die Verbindung durch die zweite Firewall zum HTTP-Server im internen Netzwerk her.

Mit den Verwaltungstools des Access Gateways hören außerdem die folgenden Ports nach Verbindungen ab:

- Port 9001: Über diesen Port erfolgen Verbindungen zum Administration Portal
- Port 9002: Über diesen Port erfolgen Verbindungen zum Administration Tool

Access Gateway in einem gesicherten Netzwerk

Sie können das Access Gateway im gesicherten Netzwerk installieren. In diesem Szenario ist in der Regel eine Firewall zwischen dem Internet und dem gesicherten Netzwerk. Das Access Gateway ist hinter der Firewall und steuert den Zugriff auf die Netzwerkressourcen.



Access Gateway in einem gesicherten Netzwerk

Access Gateway-Konnektivität in einem gesicherten Netzwerk

Wird ein Access Gateway im gesicherten Netzwerk bereitgestellt, müssen die Access Gateway Plug-in-Verbindungen die Firewall durchqueren, um eine Verbindung zum Access Gateway herstellen zu können. Standardmäßig verwenden Clientverbindungen das SSL-Protokoll auf Port 443, um diese Verbindung herzustellen. Damit diese Verbindung möglich ist, müssen Sie Port 443 in der Firewall öffnen.

Hinweis: Sie können den Port ändern, über den die Clientgeräte eine Verbindung zum Access Gateway aufbauen. Bearbeiten Sie hierzu die Porteinstellung im Administration Tool. Weitere Informationen zu dieser Porteinstellung finden Sie unter "Konfigurieren der TCP/IP-Einstellungen mit Netzwerkkabeln" auf Seite 38.

Planen für Sicherheit im Access Gateway

Beim Planen jeder Access Gateway-Bereitstellung sind gewisse grundlegende Sicherheitsaspekte im Zusammenhang mit Zertifikaten, mit der Authentifizierung und mit der Autorisierung zu beachten.

Konfigurieren der sicheren Zertifikatverwaltung

Standardmäßig enthält das Access Gateway ein selbst signiertes SSL-Serverzertifikat, mit dem das Access Gateway in der Lage ist, SSL-Handshakes zu verarbeiten. Für Testbereitstellungen sind selbst signierte Zertifikate durchaus angemessen; für den Einsatz in Produktionsumgebungen reichen diese Zertifikate jedoch nicht aus.

Citrix rät daher, vor der Bereitstellung des Access Gateways in einer Produktionsumgebung ein signiertes SSL-Serverzertifikat von einer anerkannten Zertifizierungsstelle einzuholen und auf das Access Gateway hochzuladen.

Wird das Access Gateway in einer Umgebung bereitgestellt, in der es als Client bei SSL-Handshakes fungiert (also verschlüsselte Verbindungen zu einem anderen Server einleitet), muss außerdem ein vertrauenswürdiges Stammzertifikat auf dem Access Gateway installiert werden. Weitere Informationen zu Stammzertifikaten finden Sie unter "Installieren von Stammzertifikaten auf dem Access Gateway" auf Seite 56.

Wenn Sie beispielsweise das Access Gateway mit Citrix XenApp und mit dem Webinterface installieren, können Sie Verbindungen vom Access Gateway zum Webinterface mit SSL verschlüsseln. Bei dieser Konfiguration muss ein vertrauenswürdiges Stammzertifikat auf dem Access Gateway installiert werden.

Weitere Informationen finden Sie unter "Erstellen und Installieren von Zertifikaten" auf Seite 51 und "Sichern von Verbindungen mit digitalen Zertifikaten" auf Seite 223.

Unterstützung bei der Authentifizierung

Sie können das Access Gateway so konfigurieren, dass die Benutzer authentifiziert werden und damit die Zugriffsstufe (Autorisierungsstufe) der Benutzer auf die Netzwerkressourcen im internen Netzwerk gesteuert wird.

Vor der Bereitstellung des Access Gateways sollten Sie alle Verzeichnisse und die Authentifizierungsserver in der Netzwerkumgebung einrichten, die zur Unterstützung einer der folgenden Authentifizierungsarten erforderlich sind:

- LDAP
- RADIUS
- RSA SecurID
- NTLM
- SafeWord-Produkte von Secure Computing
- Gemalto Protiva

Falls Ihre Umgebung die oben genannten Authentifizierungsarten nicht unterstützt oder nur wenige Remotebenutzer vorhanden sind, können Sie eine Liste lokaler Benutzer auf dem Access Gateway anlegen und das Access Gateway so konfigurieren, dass die Benutzer anhand dieser lokalen Liste authentifiziert werden. Bei dieser Konfiguration ist es nicht nötig, Benutzerkonten in einem separaten, externen Verzeichnis anzulegen.

Weitere Informationen zur Authentifizierung und Autorisierung finden Sie unter "Beispiele für die Konfiguration des Netzwerkzugriffs" auf Seite 241 und "Konfigurieren der Authentifizierung und Autorisierung" auf Seite 71.

Bereitstellen des Access Gateways mit Citrix XenApp oder Citrix XenDesktop

Wird das Access Gateway mit dem Ziel bereitgestellt, für sicheren Remotezugriff auf Citrix XenApp oder XenDesktop zu sorgen, ermöglicht das Access Gateway gemeinsam mit dem Webinterface und der Secure Ticket Authority (STA) den Zugriff auf veröffentlichte Anwendungen und Desktops, die in einer Serverfarm gehostet werden.

Die Konfiguration des Netzwerks Ihres Unternehmens bestimmt die Position, an der Sie das Access Gateway bereitstellen, wenn es zusammen mit einer Serverfarm genutzt werden soll. Hierbei stehen zwei Optionen zur Auswahl:

- Ist das interne Netzwerk in Ihrem Unternehmen mit einer einzelnen DMZ geschützt, stellen Sie das Access Gateway direkt in der DMZ bereit.
- Ist das interne Netzwerk in Ihrem Unternehmen dagegen mit zwei DMZs geschützt, stellen Sie je ein Access Gateway in den beiden Netzwerksegmenten in einer Double-Hop-DMZ-Konfiguration bereit. Diese Konfiguration wird nur mit Citrix XenApp unterstützt.

Weitere Informationen über die Bereitstellung des Access Gateways mit einer Serverfarm oder in einer Double-Hop-DMZ finden Sie in der *Citrix Access Gateway Standard Edition – Integrationsdokumentation für Citrix XenApp und Citrix XenDesktop*.

Bereitstellen von Access Gateway in einer Double-Hop-DMZ

Einige Unternehmen verwenden drei Firewalls zum Schutz ihrer internen Netzwerke. Diese drei Firewalls unterteilen die DMZ in zwei Bereiche, sodass ein zusätzliches Maß an Sicherheit für das interne Netzwerk erzielt wird. Diese Netzwerkkonfiguration wird als *Double-Hop-DMZ* bezeichnet.

Durch die Bereitstellung des Access Gateways in einer Double-Hop-DMZ schaffen Sie einen zentralen Zugriffspunkt auf eine Serverfarm, die sich in einem internen Netzwerk befindet. Für diese Konfiguration müssen Sie zwei Access Gateway-Geräte bereitstellen: eines in der ersten DMZ und eines in der zweiten DMZ.

Wichtig: Wird das Access Gateway in einem Double-Hop-Szenario bereitgestellt, können die Benutzer nur mit Citrix XenApp Plug-ins auf Ressourcen in einer Serverfarm zugreifen. Der Zugriff auf Ressourcen im internen Netzwerk über das Access Gateway Plug-in ist in einem Double-Hop-DMZ-Szenario nicht möglich. Es wird lediglich der ICA-Datenverkehr unterstützt.

Bereitstellen weiterer Geräte für Lastausgleich und Failover

Sie können mehrere Access Gateway-Geräte in Ihrer Umgebung installieren, um damit Folgendes zu erreichen:

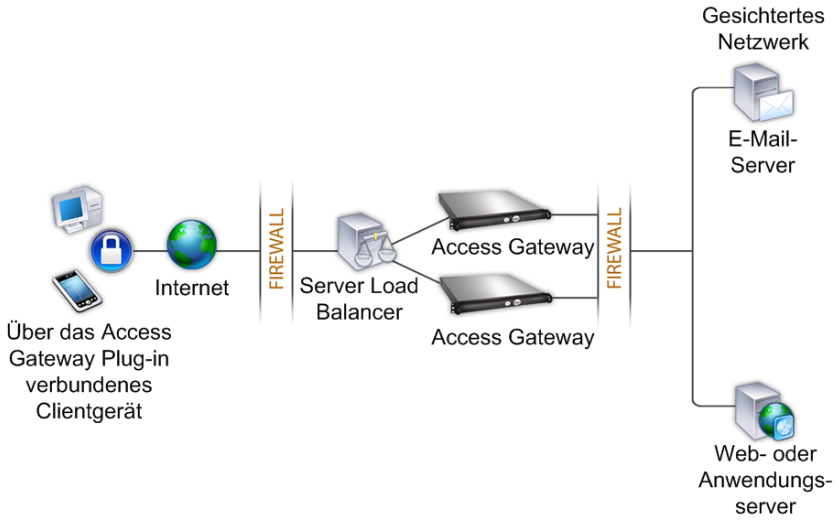
- **Skalierbarkeit:** Wenn Sie viele Remotebenutzer haben, installieren Sie zusätzliche Access Gateway-Geräte, um diese Arbeitsbelastung zu bewältigen.
- **Hohe Verfügbarkeit:** Als Vorsichtsmaßnahme für einen eventuellen Ausfall eines Access Gateways können Sie zusätzliche Access Gateway-Geräte installieren und so dafür sorgen, dass das interne Netzwerk weiterhin für die Remotebenutzer verfügbar bleibt.

Hinweis: Soll lediglich eine hohe Verfügbarkeit erzielt werden, können Sie ein Access Gateway als primäres Access Gateway konfigurieren und ein (oder mehrere) weiteres Access Gateway-Gerät als Failover-Geräte deklarieren. Bei einem Ausfall des primären Access Gateways werden die Clientverbindungen an das Failover-Access Gateway weitergeleitet. Weitere Informationen zu dieser Konfiguration finden Sie unter "Installieren zusätzlicher Access Gateway-Geräte" auf Seite 201.

Bereitstellen von Access Gateway-Geräten hinter einem Load Balancer

Um sowohl Skalierbarkeit als auch hohe Verfügbarkeit zu unterstützen, können Sie einen Load Balancer und dann mehrere Access Gateway-Geräte hinter diesem Load Balancer installieren.

Durch die Bereitstellung mehrerer Geräte hinter einem Load Balancer können Sie eine große Anzahl Remotebenutzer unterstützen und dabei die hohe Verfügbarkeit des internen Netzwerks für die Benutzer sicherstellen.



Mehrere Access Gateway-Geräte hinter einem Load Balancer

Weitere Informationen zur Bereitstellung mehrerer Access Gateway-Geräte hinter einem Load Balancer finden Sie unter "Installieren zusätzlicher Access Gateway-Geräte" auf Seite 201.

Bereitstellen von Access Gateway Advanced Edition

Access Gateway Advanced Edition besteht aus dem Access Gateway-Gerät und der Advanced Access Control-Software.

Wenn Sie Access Gateway Advanced Edition erworben haben, müssen Sie das Access Gateway so konfigurieren, dass es mit der Advanced Access Control-Software kommunizieren kann. Legen Sie mit dem Administration Tool fest, dass die Verwaltung der Einstellungen für das oder die Gatewaycluster durch Advanced Access Control erfolgen soll. Nach der Konfiguration von Advanced Access Control können Sie mit dem Administration Tool nur noch gerätespezifische Einstellungen verwalten.

Achtung: Wenn Sie festlegen, dass Advanced Access Control das Access Gateway verwalten soll, werden die entsprechenden Einstellungen im Administration Tool deaktiviert. Wurden diese Einstellungen mit dem Administration Tool konfiguriert, bevor Sie Advanced Access Control ausgewählt haben, müssen Sie diese Einstellungen mit der Access Management Console noch einmal konfigurieren. Weitere Informationen über das Konfigurieren dieser Einstellungen in der Konsole finden Sie in der Administratordokumenation von *Citrix Access Gateway Advanced Edition*. Wenn Sie die Administration mit Advanced Access Control deaktivieren, werden die Einstellungen in der Access Management Console deaktiviert und vorhandene Konfigurationswerte entfernt. Die Einstellungen, die zuvor auf dem Access Gateway konfiguriert waren, werden wiederhergestellt.

So aktivieren Sie Advanced Access Control

1. Wählen Sie auf der Registerkarte **Access Gateway Cluster** ein Access Gateway-Gerät aus und klicken Sie auf die Registerkarte **Advanced Options**.
2. Klicken Sie auf **Advanced Access Control**.
3. Geben Sie im Feld **Server running Advanced Access Control** die IP-Adresse oder den vollqualifizierten Domänennamen (FQDN) des Servers ein, auf dem die Access Management Console ausgeführt wird.
4. Wenn die Kommunikation zwischen dem Access Gateway und dem Server, auf dem Advanced Access Control ausgeführt wird, verschlüsselt werden soll, wählen Sie **Secure server communication**.
5. Klicken Sie auf **Submit**.

Die Server, die so konfiguriert sind, dass sie eine Verbindung zum Access Gateway herstellen, werden unter **Servers Running Advanced Access Control** aufgelistet. Wenn Sie einen Server aus dieser Liste entfernen möchten, wählen Sie den Server aus und klicken Sie dann auf **Remove**.

Konfigurieren mehrerer Server in einer Access-Serverfarm

Ist in der Konfiguration des Access Gateways festgelegt, dass Verbindungen mit mehreren Servern mit Access Gateway Advanced Edition aufgebaut werden sollen, wird überprüft, ob die Server tatsächlich aktiv sind, bevor das Access Gateway eine Anforderung an die Server sendet. Stellt das Access Gateway fest, dass ein Server nicht aktiv ist, wird in regelmäßigen Zeitabständen überprüft, ob der Server wieder online ist. Sie können die Zeitabstände in Sekunden angeben, in denen das Access Gateway den Server überprüft. Der Mindestzeitraum beträgt 60Sekunden.

So legen Sie das Überprüfungsintervall für einen Server mit Advanced Access Control fest

1. Klicken Sie auf die Registerkarte **Access Gateway Cluster** und anschließend auf die Registerkarte **Advanced Options**.
2. Geben Sie den gewünschten Zeitraum in das Feld **Retry invalid server in access server farm every *Zeitraum in Sekunden* seconds** ein; wobei*Zeitraum in Sekunden* das Textfeld ist und klicken Sie auf **Set**.

Erstmalige Installation des Access Gateways

Das Access Gateway kann in einer beliebigen Netzwerkinfrastruktur ohne Änderungen an der vorhandenen Hardware oder Backendsoftware installiert werden. Access Gateway kann zusammen mit anderen Netzwerkprodukten, wie z. B. Server Load Balancers, Cache-Engines, Firewalls, Routern und drahtlosen IEEE 802.11-Geräten eingesetzt werden.

Citrix empfiehlt, Access Gateway in der DMZ zu installieren. Wenn es in der DMZ installiert wird, ist das Access Gateway-Gerät Teil von zwei Netzwerken: einem privaten Netzwerk und einem öffentlichen Netzwerk mit einer öffentlich routbaren IP-Adresse. Üblicherweise ist das private Netzwerk das interne Netzwerk und das öffentliche Netzwerk das Internet. Sie können für Zugriffssteuerungs- und Sicherheitszwecke mit Access Gateway auch organisationsintern LANs partitionieren. Sie können Partitionen zwischen Kabel- oder Funknetzwerken und Daten- und Sprachnetzwerken erstellen.

Dieses Kapitel enthält:

- "Vorbereitung für die Installation von Access Gateway"
- "Einrichten der Access Gateway-Hardware"
- "Konfigurieren der TCP/IP-Einstellungen für Access Gateway"

Vorbereitung für die Installation von Access Gateway

Überprüfen Sie vor dem Installieren von Access Gateway, ob der Inhalt des Kartons mit der Packliste übereinstimmt. Sollte ein auf der Packliste genannter Gegenstand im Karton fehlen, wenden Sie sich an Citrix Customer Care.

Wenn Sie das Access Gateway in einem Rack installieren, finden Sie eine Anleitung dafür in der *Installationsübersicht für Citrix Access Gateway Standard Edition*.

Zubehör und erforderliche Informationen für die Installation

Besorgen Sie vor dem Installieren des Access Gateways alles, was für die Erstkonfiguration und den Anschluss an Ihr Netzwerk nötig ist.

Verwenden Sie für die *Erstkonfiguration* **eines** der folgenden Setups:

- Ein Kreuzkabel und einen Windows-Computer
- Zwei Netzwerkkabel, einen Netzwerkswitch und einen Windows-Computer
- Ein serielles Kabel und einen Computer mit Terminalemulationssoftware

Für den Anschluss an ein LAN benötigen Sie Folgendes:

- Ein Netzwerkkabel zum Anschluss des Access Gateways innerhalb einer Firewall oder an einen SLB
- Zwei Netzwerkkabel zum Anschluss des Access Gateways in der demilitarisierten Zone (DMZ) an das Internet und das private Netzwerk

Citrix empfiehlt, dass Sie mit der *Access Gateway Standard Edition Pre-Installation Checklist* die folgenden Netzwerkinformationen für die Geräte zusammenstellen:

- Interne IP-Adresse des Access Gateways und zugehörige Subnetzmaske
- Externe IP-Adresse des Access Gateways und zugehörige Subnetzmaske
- Vollqualifizierten Domänennamen des Access Gateways für Netzwerkadressübersetzung (NAT, Network Address Translation)
- IP-Adresse des Standardgatewaygeräts
- Für die Verbindungen zu verwendender Port

Wenn Sie das Access Gateway an einen Load Balancer anschließen, brauchen Sie die folgenden Informationen:

- IP-Adresse des Access Gateways und zugehörige Subnetzmaske
- Einstellungen des Server Load Balancers als Standardgatewaygerät (falls erforderlich). Weitere Informationen finden Sie in der Dokumentation für den Load Balancer
- Vollqualifizierten Domänennamen des Server Load Balancers, der als externe öffentliche Adresse des Access Gateways verwendet wird
- Für die Verbindungen zu verwendender Port

Hinweis: Das Access Gateway funktioniert nicht mit DHCP (Dynamic Host Configuration Protocol). Für das Access Gateway ist die Verwendung statischer IP-Adressen erforderlich.

Einrichten der Access Gateway-Hardware

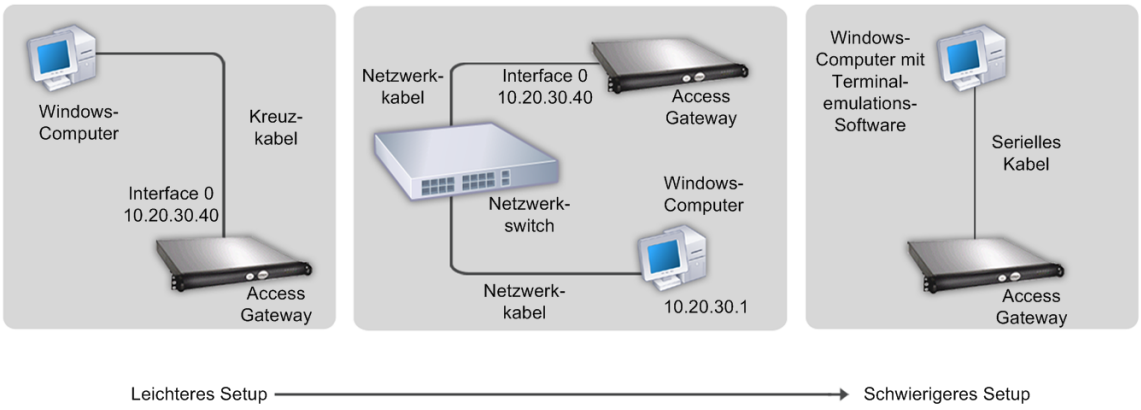
Dieser Abschnitt enthält Anweisungen für die Ersteinrichtung von Access Gateway.

So schließen Sie das Access Gateway-Gerät an

1. Installieren Sie das Access Gateway ggf. in einem Rack.

   Weitere Informationen zum Installieren des Access Gateways in einem Rack finden Sie im *Schnelleinstieg für Citrix Access Gateway Standard Edition*.

2. Stecken Sie das Stromkabel in die Steckdose.
3. Verbinden Sie das serielle Kabel mit einem Windows-Computer, ein Kreuzkabel mit einem Windows-Computer oder ein RJ-45-Netzwerkkabel mit einem Netzwerkswitch und dem Access Gateway.
4. Konfigurieren Sie die TCP/IP-Einstellungen mit den Anweisungen unter "Konfigurieren der TCP/IP-Einstellungen für Access Gateway" auf Seite 36.



Anschlussmöglichkeiten für das Access Gateway über ein Kreuzkabel, einen Netzwerkswitch oder eine Terminalemulation

Konfigurieren der TCP/IP-Einstellungen für Access Gateway

Die vorkonfigurierte IP-Adresse für Access Gateway ist 10.20.30.40. Sie können die IP-Adresse mit einem seriellen Kabel und einem Terminalemulationsprogramm ändern oder das Access Gateway mit Netzwerkkabeln verbinden und das Administration Tool verwenden. Die IP-Adresse kann mit einem seriellen Kabel und einem Terminalemulationsprogramm oder durch Anschließen des Access Gateways mit Netzwerkkabeln und dem Administration Tool geändert werden.

Konfigurieren der TCP/IP-Einstellungen mit der seriellen Konsole

Sie können die serielle Konsole verwenden, um die IP-Adresse und die Subnetzmaske der Access Gateway-Schnittstelle 0 sowie die IP-Adresse des Standardgatewaygeräts festzulegen. Alle anderen Einstellungen müssen Sie im Administration Tool konfigurieren. Sie können die serielle Konsole auch zum Testen von Verbindungen mit dem Ping-Befehl verwenden. Wenn Sie Access Gateway über die serielle Konsole erreichen möchten, bevor Sie Konfigurationseinstellungen wählen, verwenden Sie ein serielles Kabel, um das Access Gateway mit einem Computer zu verbinden, auf dem Terminalemulationssoftware ist.

Die serielle Konsole bietet die folgenden Optionen für die Konfiguration von Access Gateway:

- Mit **[0] Express Setup** konfigurieren Sie die TCP/IP-Einstellungen für Interface 0 auf der Registerkarte **Access Gateway Cluster > General Networking**.
- Mit **[1] Ping** testen Sie die Konnektivität zu anderen Netzwerkgeräten.
- Mit **[2] Link Modes** stellen Sie den Duplex- und Geschwindigkeitsmodus für Interface 0 auf der Registerkarte **Access Gateway Cluster > General Networking ein**.
- **[3] External Administration Port:** Hiermit werden Verbindungen zum Administration Tool von einem Remotecomputer aktiviert oder deaktiviert.
- Mit **[4] Display Log** können Sie das Access Gateway-Protokoll anzeigen.
- Mit **[5] Reset Certificate** setzen Sie das Zertifikat auf das Standardzertifikat zurück, das mit Access Gateway geliefert wurde.
- **[6] Change Administrative Password:** Hiermit können Sie das Standardadministratorkennwort **rootadmin** ändern.

Wichtig: Citrix empfiehlt, das Administatorkennwort zu ändern, bevor Sie Access Gateway mit Ihrem Netzwerk verbinden. Das neue Kennwort kann 6-127 ASCII-Zeichen lang sein und darf nicht mit einem Leerzeichen beginnen.

- Mit **[7] Help** zeigen Sie Hilfeinformationen an.
- **[8] Log Out:** Meldet Sie vom Access Gateway ab.

Hinweis: Citrix empfiehlt, dass Sie beide Netzwerkkarten im Gerät verwenden. Nach dem Konfigurieren der TCP/IP-Einstellungen für Interface 0 konfigurieren Sie mit dem Administration Tool die TCP/IP-Einstellungen für Interface 1.

So konfigurieren Sie TCP/IP-Einstellungen mit einem seriellen Kabel

1. Schließen Sie das serielle Kabel an den 9-poligen seriellen Anschluss am Access Gateway und an einen Computer an, auf dem eine Terminalemulationssoftware ausgeführt werden kann.
2. Starten Sie den Terminalemulator auf dem Computer, z. B. HyperTerminal.

Hinweis: HyperTerminal ist unter Windows 2000 Server, Windows Server 2003 oder Windows Server 2008 nicht automatisch installiert. Verwenden Sie die Systemsteuerung bzw. den Server-Manager, um HyperTerminal zu installieren.

3. Stellen Sie für die serielle Verbindung 9600 Bit/s, 8 Datenbits, keine Parität und 1 Stoppbit ein. Legen Sie ggf. die Hardwareflusssteuerung fest.
4. Schalten Sie das Access Gateway ein. Nach etwa drei Minuten wird auf dem Computerterminal die serielle Konsole angezeigt.
5. Wenn Sie HyperTerminal verwenden, drücken Sie nun die **Eingabetaste**.
6. Geben Sie an der seriellen Konsole die Standardanmeldeinformationen für den Administrator ein. Der Benutzername ist **root** und das Kennwort ist **rootadmin**.

Wichtig: Citrix empfiehlt, das Administratorkennwort zu ändern. Sie können hierzu das Administration Portal oder die serielle Konsole verwenden.

7. Geben Sie zum Festlegen der IP-Adresse, der Subnetzmaske und des Standardgatewaygeräts für die Schnittstelle 0 **0** ein und drücken Sie dann die Eingabetaste, um das Express Setup zu starten. Die an den einzelnen Eingabeaufforderungen eingegebenen Informationen werden angezeigt. Geben Sie zum Bestätigen Ihrer Änderungen **y** ein. Access Gateway wird neu gestartet.
8. Um zu überprüfen, ob das Access Gateway ein angeschlossenes Netzwerkgerät pingen kann, geben Sie **1** und die IP-Adresse des Geräts ein.
9. Entfernen Sie das serielle Kabel und verbinden Sie das Access Gateway über ein Kreuzkabel mit einem Windows-Computer oder über ein Netzwerkkabel mit einem Netzwerkswitch.

Weitere Access Gateway-Einstellungen werden mit dem Administration Tool konfiguriert.

Konfigurieren der TCP/IP-Einstellungen mit Netzwerkkabeln

Das Access Gateway hat zwei Netzwerkkarten. Eine Netzwerkkarte kommuniziert mit dem Internet und Clientgeräten, die nicht im gesicherten Netzwerk sind. Die andere Netzwerkkarte kommuniziert mit dem internen Netzwerk.

Citrix empfiehlt, dass beide Netzwerkkarten konfiguriert werden, um maximale Sicherheit zu erzielen. Wenn nur eine Netzwerkkarte verwendet wird, muss sie für interne Ressourcen mit Netzwerkadressenübersetzung (NAT) erreichbar sein. Außerdem wird bei Verwendung nur eines Netzwerkadapters der Datendurchsatz des Netzwerks halbiert, was zu Engpässen bei der Datenübertragung führen kann.

Sie können Access Gateway installieren und die TCP/IP-Einstellungen konfigurieren, indem Sie Netzwerkkabel (wie zwei RJ-45-Ethernet-Netzwerkkabel) oder Kreuzkabel verwenden. Die Ethernetkabel werden mit einem Netzwerkswitch und Access Gateway verbunden. Die Kreuzkabel werden mit einem Windows-Computer und Access Gateway verbunden.

Um das Access Gateway mit Kreuz- oder Ethernetkabeln zu konfigurieren, installieren Sie zuerst das Administration Tool und konfigurieren dann die Einstellungen.

So installieren Sie das Administration Tool

1. Schalten Sie das Access Gateway ein.

   Nach etwa drei Minuten ist das Access Gateway für die Erstkonfiguration in Ihrem Netzwerk bereit.

2. Öffnen Sie einen Webbrowser und geben Sie https://10.20.30.40:9001 ein, um das Administration Portal zu öffnen. Standardbenutzername und -kennwort sind **root** und **rootadmin**.

3. Klicken Sie auf der Registerkarte **Downloads** unter **Access Gateway Administration Tool** auf **Install the Access Gateway Administration Tool**.

   Folgen Sie den Anweisungen, um die Installation abzuschließen.

Nachdem das Administration Tool installiert ist, können Sie die Netzwerkeinstellungen konfigurieren.

So konfigurieren Sie die Netzwerkeinstellungen mit dem Administration Tool

1. Melden Sie sich am Administration Tool mit dem Standardbenutzernamen und -kennwort an.

2. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Access Gateway.

3. Geben Sie auf der Registerkarte **General Networking** unter **Interface 0** und **Interface 1** neben **IP Address** die neue IP-Adresse des Geräts ein.

   Citrix empfiehlt, dass Sie **Use both interfaces** auswählen.

4. Geben Sie in das Feld **Subnet mask** die Subnetzmaske für die IP-Adresse an, die Sie für die beiden Netzwerkkarten eingegeben hatten.

5. Geben Sie unter **External FQDN** den vollqualifizierten Domänennamen ein.

   Wichtig: Der FQDN muss mit dem übereinstimmen, der auf dem digitalen Zertifikat und der Lizenz für Access Gateway angegeben wurde.

6. Unter **Duplex Mode** wählen Sie die Richtung der Übertragungsdaten.

   Die Standardeinstellung ist **Auto**. Sie können auch Vollduplex und Halbduplex wählen.

7. Unter **Speed Mode** wählen Sie die Netzwerkgeschwindigkeit der Karte.

   Die Standardeinstellung ist **Auto**. Sie können auch **10 Mbps**, **100 Mbps** oder **1000 Mbps** wählen.

8. Unter **Maximum Transmission Unit (MTU)** wählen Sie die maximale Übertragungseinheit, die die maximale Größe des übertragenen Pakets bestimmt.

   Der Standardwert ist 1500.

9. Geben Sie unter **Port** den Port an, der für eingehende Verbindungen verwendet werden soll. Standardwert ist 443.

10. Wenn Sie ein Standardgateway konfigurieren möchten, geben Sie im Bereich **Default Gateway** unter **IP address** die IP-Adresse des Gateways ein. Wählen Sie unter **Interface** den Netzwerkadapter auf dem Access Gateway aus, mit dem das Standardgateway kommuniziert.

    Die IP-Adresse ist für das Standardgatewaygerät, wie der Hauptrouter, die Firewall oder der Server Load Balancer, abhängig von Ihrer Netzwerkkonfiguration. Diese IP-Adresse sollte mit der Standardgatewayeinstellung auf den Computern in demselben Subnetz übereinstimmen.

    Informationen zum Zusammenhang zwischen dem Standardgateway und dem dynamischen oder statischen Routing finden Sie unter "Konfigurieren weiterer Netzwerkeinstellungen" auf Seite 58.

11. Klicken Sie auf **Submit**, um die Konfigurationseinstellungen zu speichern.

Nachdem Sie die Netzwerkeinstellungen auf dem Access Gateway konfiguriert haben, müssen Sie das Gerät neu starten. Weitere Informationen hierzu finden Sie unter "Neustarten des Access Gateways" auf Seite 42.

Hinweis: Ein Neustart des Access Gateway-Geräts ist erst notwendig, wenn Sie alle Konfigurationsschritte vollständig ausgeführt haben. Dazu gehört die Konfiguration des Netzwerkzugriffs für das Gerät und die Installation der Zertifikate und Lizenzen. Weitere Informationen über die Konfiguration zusätzlicher Netzwerkeinstellungen finden Sie unter "Konfigurieren des Access Gateways für die Netzwerkumgebung" auf Seite 43.

Umleiten von Verbindungen auf Port 80 an einen sicheren Port

Standardmäßig lässt das Access Gateway keine unsicheren Verbindungen auf Port 80 zu. Wenn ein Benutzer versucht, mit HTTP auf Port 80 eine Verbindung zum Access Gateway herzustellen, kommt die Verbindung nicht zustande.

Sie können das Access Gateway so konfigurieren, dass HTTP-Verbindungsversuche auf Port 80 automatisch an sichere Verbindungen auf Port 443 (oder einem anderen sicheren Port) umgeleitet werden.

Wenn ein Benutzer versucht, eine unsichere Verbindung auf Port 80 herzustellen, konvertiert das Access Gateway diesen Verbindungsversuch automatisch in eine sichere (mit SSL verschlüsselte) Verbindung auf Port 443.

So leiten Sie unsichere Verbindungen um

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Access Gateway.
2. Klicken Sie auf die Registerkarte **General Networking**.
3. Klicken Sie auf **Advanced**.
4. Aktivieren Sie die Option **Redirect any requests for port 80 to a secure port** und klicken Sie auf **OK**.

Hinweis: Wenn Sie die Standardeinstellung **Do not accept connections on port 80** verwenden, schlagen alle Verbindungsversuche auf Port 80 fehl und es wird nicht versucht, sie an Port 443 umzuleiten.

Konfigurieren der TCP/IP-Einstellungen für eine Double-Hop-Bereitstellung

Das Access Gateway kann in einer Double-Hop-DMZ installiert werden, um Zugriff auf eine Serverfarm zu geben. Weitere Informationen über diese Bereitstellung finden Sie in der *Citrix Access Gateway Standard Edition – Integrationsdokumentation für Citrix XenApp und Citrix XenDesktop*.

Neustarten des Access Gateways

Starten Sie das Access Gateway nach der Konfiguration der Netzwerkeinstellungen neu.

So starten Sie das Access Gateway neu

1. Klicken Sie im Administration Tool auf die Registerkarte **Access Gateway Cluster** und öffnen Sie das Fenster für das Access Gateway.
2. Klicken Sie auf der Registerkarte **Administration** neben **Restart the appliance** auf **Restart**.

   - Oder -

   Klicken Sie im Menü **Action** auf **Restart *Gerätename***, wobei *Gerätename* der Name des Access Gateways ist.

Sie können Access Gateway auch über das Administration Portal neu starten.

So starten Sie Access Gateway über das Administration Portal neu

Klicken Sie im Administration Portal auf **Maintenance**. Klicken Sie neben **Restart the Server** auf **Restart**.

Konfigurieren des Access Gateways für die Netzwerkumgebung

Sobald Sie die grundlegenden TCP/IP-Einstellungen auf dem Access Gateway festgelegt haben, konfigurieren Sie das Gerät für Ihre Netzwerkumgebung.

Dieses Kapitel enthält:

- "Installieren von Lizenzen"
- "Erstellen und Installieren von Zertifikaten"
- "Konfigurieren weiterer Netzwerkeinstellungen"
- "Konfigurieren von Datum und Uhrzeit auf dem Access Gateway"
- "Verwenden der Standardportalseite"

Installieren von Lizenzen

Die Access Gateway-Lizenzierung begrenzt die Anzahl der gleichzeitigen Benutzersitzungen auf die Anzahl der gekauften Lizenzen. Wenn Sie also 100 Lizenzen kaufen, können 100 Benutzer gleichzeitig angemeldet sein. Sobald sich Benutzer abmelden, wird diese Lizenz für andere Benutzer freigegeben. Benutzer, die sich von mehr als einem Computer an Access Gateway anmelden, werden als zwei Benutzer gezählt und verbrauchen zwei Lizenzen.

Wenn alle Lizenzen verwendet werden, sind keine zusätzlichen Verbindungen möglich, bis ein Benutzer sich abmeldet oder der Administrator mit dem Administration Tool eine Verbindung beendet und so eine Lizenz freigibt.

Lizenzen für das Access Gateway werden mit dem Administration Tool installiert. Lizenzdateien werden auf der Basis des Hostnamens erstellt, wobei der vollqualifizierte Domänenname (FQDN) des Access Gateways verwendet wird. Das Access Gateway, auf dem die Lizenzen installiert sind (auch als *Lizenzserver* bezeichnet), verarbeitet die installierten Lizenzdateien; ungültige Lizenzdateien werden nicht berücksichtigt.

Gibt es mehrere Access Gateway-Geräte im Netzwerk, fungiert ein Access Gateway als Lizenzserver, der den anderen Geräten die Lizenzen zuweist. Sobald ein Benutzer sich an einem Gerät im Netzwerk anmeldet, wird die Lizenz von dem Access Gateway abgerufen, das als Lizenzserver dient. In einem Cluster werden die installierten Lizenzen nicht auf den anderen Geräten veröffentlicht. Weitere Informationen zur Verwendung von Lizenzen mit mehreren Geräten finden Sie unter "Konfigurieren von Lizenzen für mehrere Geräte" auf Seite 48.

Wichtig: Der Hostname in der Lizenzdatei muss genau (inklusive Groß- und Kleinschreibung) mit dem Hostnamen auf dem Access Gateway übereinstimmen.

Wenn Sie Access Gateway Advanced Edition verwenden, wird die Lizenzierung vom Citrix Lizenzserver übernommen. Weitere Informationen über die Lizenzierung mit Access Gateway Advanced Edition finden Sie im *Schnelleinstieg für die Citrix Lizenzierung* und in der Administratordokumentation für *Access Gateway Advanced Edition*.

Lizenztypen für Access Gateway

Es gibt drei Arten von Lizenzen, die auf dem Access Gateway installiert werden können:

- Die Standardlizenz wird nur bei Access Gateway Standard Edition installiert und bestimmt die Anzahl der Benutzer, die sich mit dem Access Gateway Plug-in, Citrix XenApp Plug-ins oder Citrix Desktop Receiver anmelden können.
- Die universelle Lizenz wird bei Gateway Standard Edition, Access Gateway Advanced Edition und Access Gateway Enterprise Edition installiert und bestimmt die Anzahl der Benutzer, die sich mit dem Access Gateway Plug-in, Citrix XenApp Plug-ins oder Citrix Desktop Receiver anmelden können. Die universelle Lizenz wird auch für clientlose Zugriffsverbindungen durch Access Gateway Advanced Edition und Access Gateway Enterprise Edition verwendet.
- Die XenDesktop-Verbindungslizenz wird auf dem Access Gateway installiert und bestimmt die Anzahl der zulässigen ICA-Verbindungen zum Citrix XenDesktop. Diese Lizenzen sind nur in XenDesktop Standard, Advanced und Enterprise enthalten, Stand Juni 2009. Dieser Lizenztyp wird für Citrix XenApp nicht verwendet.

Ermitteln von Lizenzierungsstatistiken

Das Administration Tool zeigt die Anzahl der Lizenzen, die von Benutzern verwendet werden. Dazu gehören Lizenzen, die von Access Gateway Plug-in- und XenDesktop-Verbindungen verwendet werden. Sie finden Lizenzierungsinformationen unter **Access Gateway Cluster**, indem Sie das Access Gateway-Fenster öffnen und auf die Registerkarten **Licensing** und **Statistics > Global** klicken.

Informationen auf der Registerkarte "Licensing"

Die Informationen auf der Registerkarte "Licensing" unter **Information about the licensing server** beziehen sich auf das Access Gateway, das als Lizenzserver fungiert. Wenn Benutzer sich mit dem Access Gateway verbinden und dafür entweder eine Access Gateway- oder XenDesktop-Verbindungslizenz verwenden, dann erscheint die Sitzung auf dieser Registerkarte. Wenn Sie mehrere Access Gateway-Geräte im Cluster haben, werden die Lizenzierungsinformationen von allen Geräten auf dieser Registerkarte aggregiert.

Die Registrierungskarte **Licensing** enthält folgende Informationen:

- **Total licenses available:** Die Zahl in diesem Feld zeigt die Gesamtzahl der Access Gateway- (Standard und Universal) und XenDesktop-Verbindungslizenzen, die auf dem Access Gateway installiert sind.
- **Total licenses in use:** Diese Zahl steht für alle derzeit verwendeten Lizenzen. Dazu gehören Access Gateway- und XenDesktop-Verbindungslizenzen.
- **ICA licenses available:** Dies ist die Gesamtzahl der XenDesktop-Verbindungslizenzen, die auf dem Access Gateway installiert sind.
- **ICA licenses in use:** Dies ist die Gesamtzahl der XenDesktop-Verbindungslizenzen, die derzeit verwendet werden.
- **Access Gateway licenses available:** Die Gesamtzahl der Standard- und universellen Lizenzen, die auf dem Access Gateway installiert sind.
- **Access Gateway licenses in use:** Die Gesamtzahl der Access Gateway-Lizenzen, die verwendet werden.

Auf der Registerkarte **Licensing** finden Sie auch Informationen zu den Lizenzen, die auf dem Access Gateway installiert sind: Dazu gehören die Gesamtzahl der Access Gateway- und XenDesktop-Verbindungslizenzen, das Ablaufdatum von Subscription Advantage, das Ausstellungs- und Verfallsdatum der Lizenzen, der Lizenztyp und die unterstützten Features.

Falls zwei Lizenzen mit derselben Seriennummer installiert sind, werden diese Dateien nicht einzeln gerechnet. Das Gerät, das als Lizenzserver fungiert, wählt eine der Lizenzdateien aus und weist den Benutzern die Lizenzen zu.

Informationen auf der Registerkarte "Statistics"

Die Lizenzierungsinformationen auf der Registerkarte **Statistics** zeigen Access Gateway- und XenDesktop-Verbindungslizenzen, die derzeit auf dem Access Gateway-Gerät verwendet werden, auf dem Sie die Daten ansehen. Die Informationen auf dieser Registerkarte müssen nicht mit den Informationen auf der Registerkarte **Licensing** übereinstimmen.

Abrufen Ihrer Lizenzdateien

Nachdem Sie Access Gateway installiert haben, können Sie Ihre Lizenzdateien von Citrix abrufen. Dazu greifen Sie unter http://www.mycitrix.com/ auf Ihre verfügbaren Lizenzen zu und generieren eine Lizenzdatei. Wenn die Lizenzdatei generiert wurde, laden Sie sie auf den Computer herunter, auf dem das Administration Tool installiert ist. Anschließend können Sie die Lizenzdatei auf das Access Gateway hochladen.

Bevor Sie auf die Citrix Website gehen, sollten Sie die folgenden Informationen haben:

- **Lizenzcode:** Sie finden den Code auf der Access Gateway-CD, in einer E-Mail von Citrix oder auf MyCitrix. Wenn Sie ein Upgrade von einer älteren Version des Access Gateways durchführen, können Sie weiterhin die vorhandene Lizenz verwenden, sofern die Lizenz über das Subscription Advantage Management Renewal Information System (SAMRI) bezogen wurde und das Subscription Advantage-Datum noch nicht abgelaufen ist.
- **Die Benutzer-ID und das Kennwort für MyCitrix:** Sie können sich auf MyCitrix für dieses Kennwort registrieren.

Hinweis: Wenn Sie diese Informationen nicht haben, wenden Sie sich bitte an Citrix Customer Care.

- **FQDN des Access Gateways:** Das Eingabefeld für diesen Namen auf MyCitrix unterscheidet zwischen Groß- und Kleinschreibung, achten Sie daher darauf, den Namen genau von der Registerkarte **Access Gateway Cluster > General Networking** zu übertragen.
- **Anzahl der Lizenzen in der Lizenzdatei:** Sie müssen nicht alle Lizenzen, auf die Sie Anspruch haben, gleichzeitig herunterladen. Wenn Ihr Unternehmen 100 Lizenz gekauft hat, können Sie beispielsweise nur 50 herunterladen. Sie können später den Rest in einer anderen Lizenzdatei zuweisen. Auf dem Access Gateway können mehrere Lizenzdateien installiert werden.

So rufen Sie Ihre Lizenzdatei ab

1. Gehen Sie zu http://www.citrix.com/ und klicken Sie auf **My Citrix**.
2. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein.

   Bei der ersten Anmeldung an der Website werden Sie aufgefordert, weitere Informationen anzugeben.
3. Zeigen Sie in **My Tools** auf **Choose a Toolbox** und klicken Sie dann auf **Activation System/Manage Licenses > View Licenses > Click to Allocate**.
4. Folgen Sie den Anweisungen, um Ihre Lizenzdatei abzurufen.

Nachdem der Download der Lizenzdatei auf Ihren Computer erfolgreich abgeschlossen wurde, können Sie die Datei auf dem Access Gateway installieren.

So installieren Sie eine Lizenz auf dem Access Gateway-Gerät

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Access Gateway.
2. Klicken Sie auf die Registerkarte **Licensing**.
3. Wählen Sie **Use this appliance as the license server**.
4. Klicken Sie neben **Install a license file** auf **Browse**, navigieren Sie zur Lizenzdatei und klicken Sie auf **Open**.
5. Klicken Sie auf der Registerkarte **General Networking** auf **Submit**, nachdem die Lizenzdatei auf das Access Gateway hochgeladen wurde.

Wichtig: Citrix empfiehlt, von allen Lizenzdateien, die Sie erhalten, jeweils eine Kopie auf dem lokalen Computer zu speichern. Wenn Sie ein Backup der Konfigurationsdatei speichern, werden alle geladenen Lizenzdateien in das Backup aufgenommen. Wenn Sie die Access Gateway-Serversoftware neu installieren müssen und kein Backup der Konfiguration haben, brauchen Sie die Originallizenzdateien.

Konfigurieren von Lizenzen für mehrere Geräte

Wenn Sie mehrere Geräte im Netzwerk installiert haben, legen Sie ein Access Gateway fest, das als Lizenzserver fungieren soll. Installieren Sie die Lizenzen auf dem Access Gateway-Gerät, das dann als Lizenzserver fungiert. Die anderen Geräte rufen die Lizenzen von diesem Access Gateway-Gerät ab. Die anderen Geräte in Ihrem Netzwerk müssen nicht Teil eines Clusters sein, um eine Verbindung zu dem Lizenzserver herstellen und eine Lizenz abrufen zu können. Die Lizenzen werden den Geräten unabhängig von ihrem jeweiligen Status im Netzwerk zugewiesen.

So rufen Sie Lizenzen vom Lizenzserver ab

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Access Gateway, das nicht als Lizenzserver fungiert.
2. Klicken Sie auf die Registerkarte **Licensing**.
3. Wählen Sie **Use a different appliance as the license server**.
4. Geben Sie unter **FQDN or IP address** den vollqualifizierten Domänennamen (FQDN) oder die IP-Adresse des Lizenzservers an.
5. Ändern Sie die Portnummern in den Feldern **Manager port** und **Vendor port** oder übernehmen Sie die Standardeinstellungen 27000 und27001.
6. Klicken Sie auf **Submit**.
7. Wiederholen Sie den Vorgang für jedes Access Gateway im Netzwerk.

Wiederholen Sie dieses Verfahren für alle Access Gateway-Geräte im Cluster, die keine Lizenzserver sind.

Der Managerport stellt den ersten Kontakt vom remoten Access Gateway her und leitet es an den Lizenzserver weiter. Dann wird die Kommunikation vom Managerport and den Vendorport übergeben. Der Vendorport wird auf dem Lizenzserver ausgeführt und gewährt die Lizenz.Dabei wird die Portnummer 27001 verwendet. Die Portnummern lassen sich an die vorliegende Firewall-Konfiguration anpassen. Der Manager-Port zeichnet die ausgecheckten Lizenzen und die Access Gateway-Geräte, auf denen sie Lizenzen verwendet werden, auf.

Unter Umständen müssen Sie neue Firewall-Regeln anlegen, damit der Netzwerkzugriff auf die Lizenzserverports möglich wird.

Herunterladen von Lizenzprotokollen

Sie können Lizenzprotokolle mit ausführlichen Informationen zur Lizenznutzung herunterladen. Die Protokolle sind nach dem Herunterladen in der komprimierten Datei license_logs.zip.

So laden Sie Lizenzprotokolle herunter

1. Wählen Sie auf der Registerkarte **Access Gateway Cluster** ein Access Gateway-Gerät aus und klicken Sie auf die Registerkarte **Licensing**.
2. Klicken Sie unter **Information about this Access Gateway** neben **Download licensing logs** auf **Download All**.
3. Legen Sie den Ordner fest, in den ZIP-Datei heruntergeladen werden soll, und klicken Sie auf **Speichern**.

Nachdem die ZIP-Datei auf Ihrem Computer gespeichert ist, können Sie die Lizenzprotokolle mit einem Komprimierungsprogramm wie WinZip extrahieren. Die Lizenzdateien (mit der Dateierweiterung .lic) lassen sich in einem Texteditor öffnen.

Aktualisieren von Lizenzierungsinformationen

Wenn Sie Änderungen an der Lizenzierung auf dem Access Gateway vornehmen, können Sie die Angaben auf der Registerkarte **Licensing** aktualisieren.

So aktualisieren Sie die Lizenzierungsinformationen

Klicken Sie unter **Information about the licensing server** auf **Refresh all information**.

Aktualisieren vorhandener Lizenzen

Als Subscription Advantage-Mitglied können Sie Ihre vorhandenen Access Gateway-Lizenzen austauschen (migrieren) und damit Ihre Lizenzdateien auf den neuesten Stand bringen.

Kulanzzeitraum für die Lizenzierung

Bei der Installation des Access Gateways beginnt ein viertägiger Kulanzzeitraum, während dessen Ihnen zwei Lizenzen zur Verfügung stehen. Die Lizenz muss auf dem Gerät vor dem Ablaufen des Kulanzzeitraums installiert sein. Sonst können Benutzer sich nicht anmelden.

Wenn der Access Gateway-Lizenzserver ausfällt, haben die anderen Geräte im Cluster einen Kulanzzeitraum von 30 Tagen. Das Access Gateway speichert das Datum, an dem zum letzten Mal eine Verbindung zum Lizenzserver hergestellt wurde. Die Benutzer können sich während dieses Kulanzzeitraums wie gewohnt anmelden. Sobald das Remotegerät den Lizenzserver erkennt, wird der dreißigtägige Kulanzzeitraum zurückgesetzt. Bei einem erneuten Ausfall des Lizenzservers erhalten die Benutzer erneut einen dreißigtägigen Kulanzzeitraum.

Testen der Lizenzinstallation

Testen Sie, ob die Lizenzierung richtig konfiguriert wurde, indem Sie einen Testbenutzer erstellen und sich dann mit dem Citrix Access Gateway Plug-in und den Anmeldeinformationen anmelden, die Sie für diesen Benutzer eingerichtet haben.

So testen Sie Ihre Konfiguration

1. Öffnen Sie das Administration Tool.
2. Klicken Sie auf die Registerkarte **Access Policy Manager**.
3. Klicken Sie mit der rechten Maustaste im linken Bereich auf den Ordner "Local Users" und klicken Sie dann auf **New User**.
4. Geben Sie im Dialogfeld **New User** in das Feld **User Name** einen Benutzernamen ein und in das Feld **Password** entsprechend das Kennwort. Wiederholen Sie die Eingabe des Kennworts im Feld **Verify Password** und klicken Sie auf **OK**.
5. Geben Sie in einem Webbrowser die Adresse des Access Gateways in Form der IP-Adresse oder als FQDN ein, um eine Verbindung zur internen oder externen Schnittstelle herzustellen. Folgende Formate werden akzeptiert: *https://IP-Adresse* oder *https://FQDN*.
6. Geben Sie auf der Seite **Citrix Access Gateway** die Anmeldeinformationen ein.
7. Klicken Sie auf der Portalseite auf **Citrix Access Gateway**.

   Wenn sich ein Benutzer das erste Mal verbindet, wird das Access Gateway Plug-in heruntergeladen und auf dem Clientgerät installiert. Nachdem die Installation abgeschlossen ist, müssen Benutzer sich noch einmal über die Webportalseite oder das Startmenü anmelden.

Die Erstkonfiguration ist damit abgeschlossen. Nach der Erstkonfiguration können Sie die zugänglichen Netzwerke konfigurieren, sodass Verbindungen zu allen Netzwerkressourcen (z. B. E-Mail, Webserver, Dateifreigaben) auf dieselbe Weise wie an Ihrem Arbeitsplatz möglich sind. Versuchen Sie zum Testen der Konfiguration, eine Verbindung zu Anwendungen und Ressourcen im gesicherten Netzwerk herzustellen.

Erstellen und Installieren von Zertifikaten

Das Access Gateway enthält ein digitales Zertifikat, das nicht von einer vertrauenswürdigen Zertifizierungsstelle signiert ist. Installieren Sie auf dem Access Gateway ein digitales X.509-Zertifikat, das zu Ihrem Unternehmen gehört und von einer Zertifizierungsstelle signiert wurde. Ihr Unternehmen kann als seine eigene Zertifizierungsstelle agieren, Sie können aber auch ein digitales Zertifikat von einer gewerblichen Zertifizierungsstelle beziehen, wie z. B. Verisign und Thawte.

Achtung: Das Betreiben des Access Gateways ohne ein von einer Zertifizierungsstelle signiertes digitales Zertifikat kann VPN-Verbindungen der Gefahr böswilliger Angriffe aussetzen.

Das Access Gateway akzeptiert Zertifikatdateien im PEM-Format (Privacy Enhanced Mail). PEM ist ein Textformat, das die Base-64-Verschlüsselung des binären DER-Formats (Distinguished Encoding Rules) darstellt. Das PEM-Format legt die Verwendung der Text-BEGIN- und -END-Zeilen fest, die die Art des verschlüsselten Inhalts angeben.

Es gibt zwei Möglichkeiten, ein sicheres Zertifikat und einen privaten Schlüssel auf dem Access Gateway zu installieren:

- Erstellen Sie mit dem Administration Tool eine Zertifikatsignier-anforderung (Certificate Signing Request, CSR). Daraufhin werden ein Zertifikat und ein privater Schlüssel erstellt. Der private Schlüssel verbleibt auf dem Access Gateway, während das Zertifikat zum Signieren an die Zertifizierungsstelle gesendet wird. Nachdem das Zertifikat zurückgesendet wurde, wird es auf dem Gerät installiert. Während der Installation wird das Zertifikat mit dem kennwortgeschützten privaten Schlüssel zusammenge-führt. Citrix empfiehlt, dieses Verfahren zum Erstellen und Installieren sicherer Zertifikate zu verwenden.

- Installieren Sie ein PEM-Zertifikat und einen privaten Schlüssel von einem Windows-Computer aus. Bei diesem Verfahren werden ein signiertes Zertifikat und ein privater Schlüssel gemeinsam hochgeladen. Das Zertifikat wird von einer Zertifizierungsstelle signiert und dann mit dem privaten Schlüssel zusammengeführt.

Übersicht über Zertifikatsignieranforderungen

Bevor Sie ein Zertifikat auf das Access Gateway hochladen können, müssen Sie eine CSR (Certificate Signing Request, Zertifikatsignieranforderung) und einen privaten Schlüssel generieren. Die CSR wird mit "Certificate Signing Request" im Administration Tool erstellt. "Certificate Signing Request" ist die Registerkarte auf der eine CSR-Datei erstellt wird. Die erstellte Datei wird per E-Mail zum Signieren an die Zertifizierungsstelle gesendet. Die Zertifizierungsstelle signiert das Zertifikat und sendet es an die angegebene E-Mail-Adresse zurück. Anschließend können Sie das Zertifikat auf dem Access Gateway installieren.

Zur sicheren Datenübertragung mit SSL/TLS muss ein Serverzertifikat auf dem Access Gateway vorliegen. So können Sie ein Serverzertifikat abrufen und auf dem Access Gateway installieren:

- Erstellen Sie eine CSR (myserver.csr) auf der Registerkarte "Certificate Signing Request" im Administration Tool.
- Senden Sie die Datei myserver.csr per E-Mail an einen autorisierten Zertifikatsanbieter.
- Sobald Sie die signierte Zertifikatdatei von der Zertifizierungsstelle erhalten, laden Sie das Zertifikat mit dem Administration Tool hoch. Das Administration Tool wandelt das Zertifikat automatisch in das vom Access Gateway geforderte PEM-Format um.

Kennwortgeschützte private Schlüssel

Die mit der Zertifikatsignieranforderung erstellten privaten Schlüssel werden verschlüsselt und kennwortgeschützt auf dem Access Gateway gespeichert. Beim Erstellen der Zertifikatsignieranforderung werden Sie aufgefordert, ein Kennwort für den privaten Schlüssel festzulegen. Dieses Kennwort schützt den privaten Schlüssel vor Manipulationen und ist außerdem beim Wiederherstellen einer gespeicherten Konfiguration auf dem Access Gateway erforderlich. Kennwörter werden in jedem Fall verwendet, unabhängig davon, ob der private Schlüssel verschlüsselt ist.

So erstellen Sie eine Zertifikatsignieranforderung

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Gerät.
2. Geben Sie auf der Registerkarte **Certificate Signing Request** die erforderlichen Informationen ein und klicken Sie dann auf **Generate Request**.

   Hinweis: Geben Sie in das Feld **Access Gateway FQDN** den vollqualifizierten Domänennamen ein, der auf der Registerkarte **General Networking** aufgeführt ist. Geben Sie unter **Password** das Kennwort für den privaten Schlüssel ein.

3. Es wird eine CSR-Datei erstellt. Speichern Sie die CSR-Datei auf dem lokalen Computer.
4. Senden Sie das Zertifikat per E-Mail an die Zertifizierungsstelle.

   Der Zertifikatsanbieter sendet Ihnen per E-Mail ein signiertes Zertifikat zurück. Installieren Sie dieses signierte Zertifikat auf dem Access Gateway.

Hinweis: Beim Speichern der Access Gateway-Konfiguration werden auch alle bereits installierten Zertifikate mit gesichert.

Nachdem Sie die Zertifikatsanforderung an die Zertifizierungsstelle gesendet haben, führen Sie die nachfolgenden Aufgaben auf dem Access Gateway erst dann wieder aus, wenn Sie das signierte Zertifikat auf dem Gerät installiert haben:

- Erstellen einer weiteren Zertifikatsignieranforderung
- Hochladen einer gespeicherten Konfigurationsdatei
- Veröffentlichen von Konfigurationseinstellungen von einem anderen Gerät im Cluster

Wichtig: Wenn Sie ein Zertifikat erstellt und an die Zertifizierungsstelle gesendet haben, erstellen Sie keine weitere Zertifikatsignieranforderung. Das Access Gateway kann nur einen privaten Schlüssel speichern. Wird die Zertifikatsignieranforderung erneut ausgeführt, wird der private Schlüssel überschrieben und das signierte Zertifikat findet keinen passenden Schlüssel als Gegenstück.

So installieren Sie eine Zertifikatdatei mit dem Administration Tool

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Gerät.
2. Klicken Sie auf der Registerkarte **Administration** neben **Upload a .crt signed certificate** auf **Browse**.

   Diese Schaltfläche kommt nur dann zum Einsatz, wenn Sie ein signiertes Zertifikat installieren, das über die Registerkarte **Certificate Signing Request** erstellt wurde.
3. Suchen Sie die Datei, die hochgeladen werden soll, und klicken Sie auf **Öffnen**.

Sie können das Zertifikat auch über das Administration Portal hochladen.

So installieren Sie ein Zertifikat über das Administration Portal

1. Klicken Sie auf der **Administration Portal**-Hauptseite auf **Maintenance**.
2. Klicken Sie neben **Upload Signed Certificate (.crt)** auf **Browse**.
3. Navigieren Sie zum Zertifikat und laden Sie die Datei hoch.

Zurücksetzen des Zertifikats auf die Standardversion

Das Access Gateway enthält ein Zertifikat, das keine digitale Signatur einer Zertifizierungsstelle trägt. Für den Fall, dass die Konfiguration des Geräts wiederhergestellt werden muss, können Sie das Zertifikat auf das Standardzertifikat aus dem Lieferumfang des Access Gateways zurücksetzen. Wählen Sie hierzu in der seriellen Konsole die Option zum Zurücksetzen des Zertifikats.

So setzen Sie das Zertifikat auf die Standardversion zurück

1. Schließen Sie das serielle Kabel an den 9-poligen seriellen Anschluss am Access Gateway und an einen Computer an, auf dem eine Terminalemulationssoftware ausgeführt werden kann.
2. Starten Sie den Terminalemulator auf dem Computer, z. B. HyperTerminal.

   Hinweis: HyperTerminal ist unter Windows 2000 Server, Windows Server 2003 oder Windows Server 2008 nicht automatisch installiert. Verwenden Sie die Systemsteuerung bzw. den Server-Manager, um HyperTerminal zu installieren.
3. Stellen Sie für die serielle Verbindung 9600 Bit/s, 8 Datenbits, keine Parität und 1 Stoppbit ein. Legen Sie ggf. die Hardwareflusssteuerung fest.

4. Schalten Sie das Access Gateway ein. Nach etwa drei Minuten wird auf dem Computerterminal die serielle Konsole angezeigt.
5. Wenn Sie HyperTerminal verwenden, drücken Sie die Eingabetaste und melden sich mit dem Standardbenutzernamen und den Standardkennwort **root** und **rootadmin** an.
6. Um das Zertifikat auf das Standardzertifikat zurückzusetzen, geben Sie **5** ein und drücken Sie die **Eingabetaste**.

Installieren eines Zertifikats und eines privaten Schlüssels von einem Windows-Computer aus

Wenn Sie einen Load Balancer einsetzen oder ein signiertes digitales Zertifikat mit einem privaten Schlüssel besitzen, das auf einem Windows-Computer gespeichert ist, können Sie dieses Zertifikat auf das Access Gateway hochladen. Befindet sich das Access Gateway nicht hinter einem Load Balancer, muss das Zertifikat den vollqualifizierten Domänennamen des Access Gateways aufweisen. Falls das Access Gateway hinter einem Load Balancer bereitgestellt ist, müssen alle Geräte dasselbe Zertifikat und denselben privaten Schlüssel enthalten. Weitere Informationen hierzu finden Sie unter "Konfigurieren mehrerer Geräte für die Verwendung eines Load Balancers" auf Seite 206.

So installieren Sie ein Zertifikat und einen privaten Schlüssel von einem Windows-Computer aus

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Gerät.
2. Klicken Sie auf die Registerkarte **Administration**.
3. Klicken Sie neben **Upload a .pem private key and signed certificate** auf **Browse**.
4. Gehen Sie zum Zertifikat und klicken Sie auf **Öffnen**.

   Beim Hochladen des Zertifikats auf das Access Gateway werden Sie aufgefordert, ein Kennwort festzulegen, mit dem der private Schlüssel verschlüsselt werden soll.

Installieren von Stammzertifikaten auf dem Access Gateway

Stammzertifikate werden von der Zertifizierungsstelle (CA) bereitgestellt und von SSL-Clients zur Überprüfung von Zertifikaten verwendet, die dem SSL-Server präsentiert werden. Wenn ein SSL-Client versucht, eine Verbindung mit einem SSL-Server herzustellen, präsentiert der Server ein Zertifikat. Das Clientgerät schlägt daraufhin im Stammzertifikatspeicher nach, ob das vom SSL-Server vorgelegte Zertifikat von einer Zertifizierungsstelle signiert ist, die für das Stammzertifikat als vertrauenswürdig gilt. Wird das Access Gateway in einer Umgebung bereitgestellt, in der es als Client bei SSL-Handshakes fungiert (also verschlüsselte Verbindungen zu einem anderen Server einleitet), installieren Sie ein vertrauenswürdiges Stammzertifikat auf dem Access Gateway.

Wenn Sie beispielsweise das Access Gateway mit Citrix XenApp und mit dem Webinterface installieren, können Sie Verbindungen vom Access Gateway zum Webinterface mit SSL verschlüsseln. Bei dieser Konfiguration muss ein vertrauenswürdiges Stammzertifikat auf dem Access Gateway installiert werden.

Das auf dem Access Gateway installierte Stammzertifikat muss im PEM-Format vorliegen. Unter Windows werden Stammzertifikate im PEM-Format gelegentlich mit der Dateinamenerweiterung .cer gekennzeichnet.

Sollen Zertifikate für interne Verbindungen validiert werden, muss auf dem Access Gateway ein Stammzertifikat installiert sein.

So installieren Sie ein Stammzertifikat auf dem Access Gateway

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Gerät.
2. Klicken Sie auf der Registerkarte **Administration** neben **Manage trusted root certificates** auf **Manage**.
3. Klicken Sie auf der Registerkarte **Manage** auf **Upload Trusted Root Certificate**.
4. Navigieren Sie zur Datei und klicken Sie auf **Öffnen**.

Mit **Remove Trusted Root Certificate** können Sie das Stammzertifikat wieder entfernen.

Installieren mehrerer Stammzertifikate

Es ist möglich, mehrere Stammzertifikate auf dem Access Gateway zu installieren; diese Zertifikate müssen sich allerdings in einer einzigen Datei befinden. Beispiel: Sie können eine Textdatei in einem Texteditor erstellen, die alle Stammzertifikate enthält. Öffnen Sie die einzelnen Stammzertifikate in einer anderen Instanz des Texteditors. Kopieren Sie den Inhalt der Zertifikate und fügen Sie diesen kopierten Inhalt jeweils unterhalb der letzten Zeile in die neue Textdatei ein. Sobald Sie alle Zertifikate in die neue Textdatei kopiert haben, speichern Sie die Datei im PEM-Format und laden Sie sie auf das Access Gateway hoch.

Erstellen von Stammzertifikaten über eine Eingabeaufforderung

Alternativ können Sie Stammzertifikate im PEM-Format über eine DOS-Eingabeaufforderung erstellen. Wenn Sie drei PEM-Stammzertifikate besitzen, können Sie beispielsweise mit dem nachstehenden Befehl eine einzige Datei mit allen drei Zertifikaten erstellen.

```
type root1.pem root2.pem root3.pem > current-roots.pem
```

Sollen weitere Stammzertifikate in eine vorhandene Datei eingefügt werden, verwenden Sie folgenden Befehl:

```
type root4.pem root5.pem >> current-roots.pem
```

Nach der Ausführung dieses Befehls befinden sich alle fünf Stammzertifikate in der Datei current-roots.pem. Mit dem zweifachen Größer-als-Zeichen (>>) wird der Inhalt der Dateien root4.pem und root5.pem an den bereits vorhandenen Inhalt der Datei current-roots.pem angehängt.

Konfigurieren weiterer Netzwerkeinstellungen

Nach der Installation der Lizenzen und Zertifikate auf dem Access Gateway fallen ggf. weitere Konfigurationsschritte an, mit denen das Access Gateway auf die Arbeit im Netzwerk vorbereitet wird. Dazu gehören folgende Einstellungen:

- Konfigurieren von Namensdienstanbietern, mit denen bis zu drei DNS-Server und ein WINS-Server konfiguriert werden können
- Bearbeiten der HOSTS-Datei zum Umgehen des DNS und zum Auflösen bestimmter IP-Adressen in bestimme Hostnamen
- Konfigurieren des dynamischen und statischen Routing für das Abhören von Routen, die von den Routingservern veröffentlicht werden, bzw. für die Verwendung statischer Routen
- Konfigurieren von Datum und Uhrzeit
- Konfigurieren des Standardanmeldeseite für das Access Gateway Plug-in

Konfigurieren von Namensdienstanbietern

Die Namensauflösung wird auf der Registerkarte **Name Service Providers** konfiguriert. Hier können Sie Einstellungen für bis zu drei DNS-Server und einen WINS-Server angeben.

So legen Sie DNS- und WINS-Server fest

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Gerät.
2. Klicken Sie auf die Registerkarte **Name Service Providers**.
3. Geben Sie unter **First DNS server**, **Second DNS Server** oder **Third DNS server** die IP-Adresse der einzelnen Server ein.
4. Geben Sie in das Feld **DNS suffixes** die Suffixe der Server ein.

   Dies sind die DNS-Suffixe der Server. Die einzelnen Einträge in der Liste sind durch ein Leerzeichen voneinander getrennt. Die Syntax für die Einträge lautet: *site.com*. Stellen Sie den Suffixen keinen Punkt (.) voran (Beispiel: .site.com).

   Standardmäßig überprüft das Access Gateway lediglich das Remote-DNS des Benutzers. Wenn ein Failover auf das lokale DNS des Benutzers möglich sein soll, muss Split DNS zugelassen werden. Weitere Informationen finden Sie unter "Split DNS aktivieren" auf Seite 161.
5. Geben Sie in das Feld **WINS Server** die IP-Adresse des Servers ein.
6. Klicken Sie auf **Submit**.

Bearbeiten der HOSTS-Datei

Auf der Registerkarte **Name Service Providers** können Sie Einträge in die HOSTS-Datei des Access Gateways einfügen. Mit den Einträgen in der HOSTS-Datei löst das Access Gateway die vollqualifizierten Domänennamen in IP-Adressen auf.

Beim Umwandeln eines vollqualifizierten Domänennamen in eine IP-Adresse überprüft das Access Gateway zunächst die HOSTS-Datei, bevor eine Verbindung zum DNS-Server aufgebaut wird, um die Adressübersetzung durchzuführen. Wenn der vollqualifizierte Domänenname schon mit den Angaben in der HOSTS-Datei in eine IP-Adresse aufgelöst werden kann, wird der DNS-Server gar nicht erst aufgerufen.

Für den Fall, dass das Access Gateway aufgrund der Netzwerkkonfiguration nicht auf den DNS-Server zugreifen kann, sollten Sie die entsprechenden Einträge in die HOSTS-Datei aufnehmen, damit die Adressauflösung reibungslos abläuft. Dies kann sich außerdem positiv auf die Leistung auswirken, weil das Access Gateway keine Verbindung zu einem anderen Server aufbauen muss, um die Adressen zu übersetzen.

So fügen Sie der HOSTS-Datei einen Eintrag hinzu

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Gerät.
2. Klicken Sie auf die Registerkarte **Name Service Providers**.
3. Geben Sie unter **Edit the HOSTS file** in das Feld **IP address** die IP-Adresse ein, die einem bestimmten vollqualifizierten Domänennamen zugewiesen werden soll.
4. Geben Sie in das Feld **FQDN** den vollqualifizierten Domänennamen ein, den Sie mit der im vorigen Schritt eingegebenen IP-Adresse verknüpfen möchten und klicken Sie auf **Add**.

   Die Gruppe aus IP-Adresse und HOSTS-Name wird in der Hosttabelle aufgeführt.

So entfernen Sie einen Eintrag aus der HOSTS-Datei

1. Klicken Sie unter **Host Table** auf die Gruppe aus IP-Adresse und HOSTS-Name, die Sie löschen möchten.
2. Klicken Sie auf **Remove**.

Konfigurieren von dynamischen und statischen Routen

Sie können das Access Gateway für das dynamische oder statische Routing konfigurieren. Das Access Gateway unterstützt das dynamische Routing mit dem Routing Information Protocol (RIP und RIP2).

Aktivieren von dynamischem Routing

Wenn Sie dynamisches Routing für das Access Gateway konfigurieren, passiert Folgendes:

- Das Access Gateway hört Routinginformationen ab, die in Form von RIP-UDP-Paketen veröffentlicht werden. Das Access Gateway füllt die Routingtabelle mit den RIP-Daten.
- Alle vorhandenen statischen Routen werden deaktiviert.

Beim dynamischen Routing können Sie festlegen, dass das dynamische Gateway die Festlegung des vom Access Gateway verwendeten Standardgateways durch RIP zulassen soll. Ist es aktiviert, verwendet das Access Gateway nicht das Standardgateway, das auf der Registerkarte **General Networking** für das ausgewählte Gerät unter **Access Gateway Cluster** im Administration Tool angegeben wurde.

So aktivieren Sie dynamisches Routing

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Gerät.
2. Klicken Sie auf die Registerkarte **Routes**.
3. Wählen Sie unter **Select routing type** die Option **Dynamic routing (RIP)**.
4. Klicken Sie auf **Enable dynamic gateway**, wenn das von den Routingservern bereitgestellte Standardgateway verwendet werden soll.
5. Wählen Sie unter **Routing Interface** den oder die Access Gateway-Netzwerkadapter aus, der oder die für das dynamische Routing verwendet werden soll(en).

   In der Regel befinden sich die Routingserver innerhalb der Firewall, sodass Sie für diese Einstellung den internen Netzwerkadapter (Interface 1) wählen sollten.
6. Klicken Sie auf **Submit**.

Dynamische Routen werden nicht in der Access Gateway-Routingtabelle aufgeführt.

Aktivieren der RIP-Authentifizierung für das dynamische Routing

Zur Erhöhung der Sicherheit bei dynamischem Routing können Sie das Access Gateway für die RIP-Authentifizierung konfigurieren.

Hinweis: Der RIP-Server muss RIP 2-Pakete für die RIP-Authentifizierung übertragen. RIP 1 unterstützt keine Authentifizierung.

Bei der RIP-Authentifizierung müssen sowohl der RIP-Server als auch das Access Gateway so konfiguriert werden, dass eine bestimmte Authentifizierungs-Zeichenfolge verwendet wird. Der RIP-Server kann diese Zeichenfolge wahlweise als einfachen Text versenden oder auch mit MD5 verschlüsseln.

Falls der RIP-Server die Authentifizierungs-Zeichenfolge mit MD5 verschlüsselt, muss entsprechend die Option für MD5 auf dem Access Gateway aktiviert werden.

Sie können das Access Gateway so konfigurieren, dass es Interface 0 und/oder Interface 1 nach der Zeichenfolge für die RIP-Authentifizierung abhört.

So aktivieren Sie die RIP-Authentifizierung für dynamisches Routing

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Gerät.
2. Klicken Sie auf die Registerkarte **Routes**.
3. Legen Sie die Schnittstelle(n) fest, die das Access Gateway nach der Zeichenfolge für die RIP-Authentifizierung abhören soll. Wählen Sie hierzu unter **Routing Interface** die Option **Interface 0**, **Interface 1** oder **Both**.
4. Wählen Sie **RIP Authentication String for Interface**.
5. Geben Sie in das Textfeld die Authentifizierungs-Zeichenfolge ein, die der RIP-Server übermittelt. Achten Sie dabei auf die exakte Schreibweise und auf die Groß- und Kleinschreibung.
6. Falls der RIP-Server die Authentifizierungs-Zeichenfolge mit MD5 verschlüsselt, aktivieren Sie **Enable RIP MD5 Authentication for Interface**.

   Aktivieren Sie diese Option nicht, wenn der RIP-Server die Authentifizierungs-Zeichenfolge als reinen Text übermittelt.
7. Klicken Sie auf **Submit**.

Wechseln von dynamischem Routing zu statischem Routing

Bevor Sie von dynamischem Routing zu statischem Routing wechseln, sollten Sie die dynamischen Routen in der statischen Routentabelle speichern. Mit dieser Option werden die aktuellen RIP-Daten zum dynamischen Routing als statische Routen gespeichert.

Wenn Sie von dynamischem Routing zu statischem Routing wechseln und zuvor statische Routen erstellt hatten, werden die statischen Routen in der Routingtabelle des Access Gateways aufgeführt.

Für den Fall, dass diese statischen Routen nicht mehr gültig sind oder noch keine statischen Routen erstellt wurden, geht unter Umständen der Remotezugriff auf das Administration Tool verloren. Die Benutzer können außerdem erst dann wieder auf die Ressourcen im internen Netzwerk zugreifen, wenn Sie die statischen Routen manuell konfiguriert haben.

Durch das Speichern der aktuellen RIP-Daten zum dynamischen Routing wird die Konnektivität beim Wechsel vom dynamischen Routing zum statischen Routing so lange aufrechterhalten, bis Sie die statischen Routen ordnungsgemäß konfiguriert haben.

So speichern Sie dynamische Routen in der Tabelle mit den statischen Routen

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Gerät.
2. Klicken Sie auf die Registerkarte **Routes**.
3. Klicken Sie auf **Save to Static Routes**.

Sobald die dynamischen Routen gespeichert sind, können Sie zum statischen Routing wechseln.

Konfigurieren einer statischen Route

Beim Einrichten der Kommunikation mit einem anderen Host oder Netzwerk muss u. U. eine statische Route vom Access Gateway dem neuen Ziel hinzugefügt werden, sofern Sie kein dynamisches Routing verwenden.

Richten Sie die statischen Routen auf dem Access Gateway-Adapter ein, der nicht von dem auf der Registerkarte **General Networking** angegebenen Standardgateway verwendet wird.

Ein Beispiel für das Einrichten einer statischen Route finden Sie unter "Beispiel für eine statische Route" auf Seite 64.

So fügen Sie eine statische Route hinzu

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Gerät und klicken Sie auf die Registerkarte **Routes**.
2. Wählen Sie unter **Select routing type** die Option **Static routing**.
3. Geben Sie unter **Add a static route** im Feld **Destination LAN IP address** die IP-Adresse des Ziel-LANs ein.
4. Geben Sie unter **Subnet mask** die Subnetzmaske für das Gatewaygerät ein.
5. Geben Sie unter **Gateway** die IP-Adresse für das Standardgateway ein. Wenn Sie kein Gateway angeben, kann das Access Gateway nur auf den Inhalt im lokalen Netzwerk zugreifen.
6. Wählen Sie unter **Interface** den Netzwerkadapter für die statische Route aus. Die Standardeinstellung ist Interface 0.
7. Klicken Sie auf **Hinzufügen**.

   Der Routenname wird auf der Registerkarte **Routes** in der Liste **Static routes** angezeigt.

So testen Sie eine statische Route

1. Öffnen Sie im Administration Tool auf der Registerkarte **Access Gateway Cluster** das Fenster für das Gerät.
2. Geben Sie auf der Registerkarte **Net Tools > Ping** in das Feld **Host address** die IP-Adresse des Netzwerks oder Geräts ein, dass Sie testen möchten und klicken Sie auf **Ping**.

   Wenn eine erfolgreiche Kommunikation mit dem anderen Gerät zustande kommt, wird eine entsprechende Meldung eingeblendet, dass die gleiche Anzahl von Paketen gesendet und empfangen wurde und keine Pakete verloren gegangen sind.

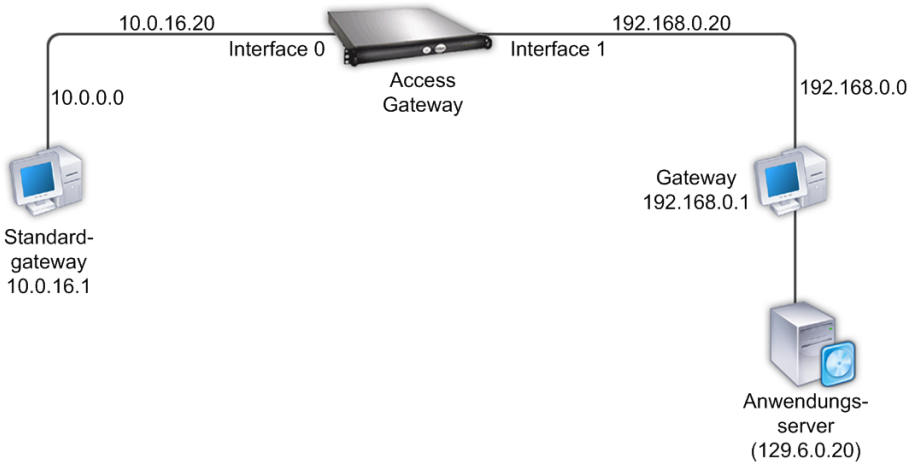
   Wenn keine Kommunikation mit dem anderen Gerät zustande kommt, erhalten Sie Statusmeldungen, aus denen hervorgeht, dass keine Pakete empfangen wurden und dass alle Pakete verloren gegangen sind. Zur Behebung dieses Problems fügen Sie erneut eine statische Route hinzu.

So entfernen Sie eine statische Route

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Gerät.
2. Klicken Sie auf die Registerkarte **Routes**.
3. Wählen Sie in der Tabelle **Static Routes** alle Routen aus, die Sie löschen möchten.
4. Klicken Sie auf **Remove Route**.

Beispiel für eine statische Route

Angenommen, die IP-Adresse für das Interface 0 am Access Gateway ist 10.0.16.20 und es liegt eine Anforderung für den Zugriff auf Daten auf 129.6.0.20 vor, wofür derzeit kein Pfad vorhanden ist. Vom Netzwerkadapter aus, der nicht als Access Gateway-Standardgateway festgelegt ist, können Sie eine statische Route zur angeforderten Netzwerkadresse erstellen. Die folgende Abbildung enthält eine grafische Darstellung dieser Situation:



Netzwerktopologie mit einer statischen Route

Die Abbildung zeigt die folgenden Verbindungen:

- Der Adapter für Interface 0 (10.0.16.20) führt zum Standardgateway (10.0.16.1), das mit dem übrigen Teil des Netzwerks 10.0.0.0 verbunden ist.
- Der Adapter für Interface 1 (192.168.0.20) ist für die Kommunikation mit dem Netzwerk 192.168.0.0 und dem zugehörigen Gateway (192.168.0.1) eingerichtet. Über dieses Gateway kann das Interface 1 mit dem Netzwerk 129.6.0.20 und dem Server an der IP-Adresse 129.6.0.20 kommunizieren.

Zum Einrichten der statischen Route müssen Sie den Pfad zwischen Interface 1 und der IP-Adresse 129.6.0.20 erstellen.

So richten Sie die statische Beispielroute ein

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Gerät.
2. Klicken Sie auf die Registerkarte **Routes**.
3. Wählen Sie ggf. unter **Select routing type** die Option **Static routing**.
4. Legen Sie im Feld **Destination LAN IP address** als IP-Adresse des Ziel-LANs **129.6.0.0** fest.
5. Legen Sie unter **Subnet Mask** die Subnetzmaske für das Gatewaygerät fest.
6. Legen Sie unter **Gateway** als IP-Adresse des Standardgateways **192.168.0.1** fest.
7. Wählen Sie unter **Interface** als Gateway-Geräteadapter die Option **Interface 1** und klicken Sie auf **Add**.

Konfigurieren von Datum und Uhrzeit auf dem Access Gateway

Die Systemzeit wird auf der Registerkarte **Date** im Administration Tool angezeigt.

So ändern Sie das Systemdatum und die Systemuhrzeit

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Gerät.
2. Klicken Sie auf die Registerkarte **Date**.
3. Aktivieren Sie unter **Synchronization mode** die Option **Manual**.
4. Geben Sie unter **Date** das Datum und die Uhrzeit ein.
5. Wählen Sie unter **Time zone** eine Zeitzone aus und klicken Sie auf **Submit**.

Konfigurieren eines NTP-Servers

Das Network Time Protocol (NTP) sendet und empfängt Zeitinformationen über TCP/IP-Netzwerke. Es eignet sich daher für die Synchronisierung der internen Uhr von Computern im Netzwerk auf der Basis einer gemeinsamen Referenzzeit.

Wenn sich in Ihrem sicheren Netzwerk ein NTP-Server befindet, können Sie das Access Gateway mit dem Administration Tool so konfigurieren, dass die Uhrzeit des Geräts mit der vom NTP-Server bereitgestellten Zeit synchronisiert wird.

So synchronisieren Sie das Access Gateway mit einem NTP-Server

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Gerät.
2. Klicken Sie auf die Registerkarte **Date**.
3. Aktivieren Sie unter **Synchronization Mode** die Option **Network Time Protocol (NTP)**.
4. Geben Sie in das Feld **NTP server** den vollqualifizierten Domänennamen des Servers ein.
5. Wählen Sie unter **Synchronization interval** einen Zeitplan für die Updates und klicken Sie auf **Submit**.

Verwenden der Standardportalseite

Die Standardportalseite ist eine HTML-Seite, auf der Benutzer die Art der Verbindung auswählen können, die von einem Remotecomputer aus hergestellt werden soll. Die Benutzer können die Verbindung entweder von der Webportalseite aus herstellen oder den Access Gateway Plug-in verwenden, der auf ihren Computern installiert ist.

Weitere Informationen zu den Anmeldeseiten und den verschiedenen Möglichkeiten zum Aufbauen einer Verbindung durch die Benutzer finden Sie unter "Konfigurieren von Anmelde- und Portalseiten für das Citrix Access Gateway Plug-in" auf Seite 171.

Von der Webportalseite aus starten Benutzer das Secure Access. Das Secure Access ist für Verbindungen von privaten Computern aus gedacht, weil die Daten aus dem Netzwerk, zu dem Benutzer eine Verbindung herstellen, an die Computer der Benutzer übertragen werden.

So stellen Sie eine Verbindung von der Standardportalseite aus her

1. Geben Sie in einem Webbrowser die Webadresse des Access Gateways ein (z. B. https://vpn.meinefirma.com).
2. Geben Sie auf der Anmeldeseite den Benutzernamen und das Kennwort ein und klicken Sie dann auf **Login**.

   Die Standardportalseite wird geöffnet.

Hinweis: Ist die Option **Enable logon page authentication** auf der Registerkarte **Global Cluster Policies** nicht aktiviert, melden sich die Benutzer erst dann an, wenn die Verbindung zur Portalseite aufgebaut ist (siehe Schritt3).

---

3. Um eine Verbindung mit dem Access Gateway Plug-in von einem gesicherten Computer herzustellen, gehen Sie wie folgt vor:

   - Klicken Sie auf **Citrix Access Gateway**.

     Wenn zum ersten Mal eine Verbindung über den Webbrowser hergestellt wird, werden Sie aufgefordert, dass Access Gateway Plug-in zu installieren.

   - Klicken Sie zweimal auf **Run**, klicken Sie auf **Next** und folgen Sie dann den Anweisungen im Installationsassistenten für das Access Gateway Plug-in.

     Das Access Gateway Plug-in wird auf dem Clientgerät installiert. Wenn das Plug-in installiert ist, können Benutzer beim nächsten Mal das Access Gateway Plug-in starten, ohne über die Webanmelde- und Portalseiten gehen zu müssen. Klicken Sie auf **Start > Alle Programme > Citrix > Citrix Access Clients > Citrix Access Gateway**, um die Verbindung herzustellen.

4. Klicken Sie auf **Citrix XenApp**, um sich am Webinterface anzumelden.

   Die Benutzer geben ihren Benutzernamen und das Kennwort ein und klicken dann auf **Anmelden**. Benutzer haben Zugriff auf in Citrix XenApp veröffentlichte Anwendungen und können Anwendungen wie Word und Outlook verwenden, als wenn sie lokal auf ihrem Computer installiert wären.

Wenn Sie das Secure Access für die automatische Anmeldung an Windows konfiguriert haben, wird das Plug-in gestartet, sobald die Benutzer ihre Windows-Anmeldeinformationen eingegeben haben. Diese Anmeldeinformationen werden auch für das Secure Access verwendet. Das bedeutet, dass die Benutzer beim Starten des Clientgeräts die Authentifizierung nicht wiederholen müssen, um eine Verbindung herzustellen, vorausgesetzt, die Benutzer haben eine Netzwerkverbindung und sie können sich an Windows anmelden. Weitere Informationen zur Konfiguration der Single Sign-On-Funktion unter Windows finden Sie unter "Konfigurieren von Single Sign-on für Windows-Betriebssysteme" auf Seite 148.

Konfigurieren des Netzwerkzugriffs

Nachdem das Gerät für den Betrieb in der Netzwerkumgebung konfiguriert wurde, konfigurieren Sie den Netzwerkzugriff für das Gerät sowie für die Gruppen und Benutzer.

So konfigurieren Sie den Netzwerkzugriff

- **Schritt 1: Konfigurieren der Netzwerke, zu denen die Clients eine Verbindung aufbauen können.** Standardmäßig können die Clients keine Verbindungen zu einem Netzwerk herstellen. Als ersten Schritt beim Konfigurieren des Netzwerkzugriffs legen Sie auf der Registerkarte **Global Cluster Policies** die Netzwerke fest, zu denen die Clients eine Verbindung herstellen sollen.
- **Schritt 2: Konfigurieren der Authentifizierung und Autorisierung.** Mit der Authentifizierung wird definiert, wie die Benutzer sich anmelden; die Konfiguration erfolgt mit Bereichen (realms). Zu den Authentifizierungstypen gehören lokal, NTLM, LDAP, RADIUS, RSA SecurID, Gemalto Protiva und Secure Computing SafeWord. Bei der Autorisierung stehen die folgenden Optionen zur Verfügung: lokal, LDAP, RADIUS, NTLM, keine Autorisierung. Weitere Informationen zur Konfiguration der Authentifizierung und Autorisierung finden Sie unter "Konfigurieren der Authentifizierung und Autorisierung" auf Seite 71.
- **Schritt 3: Konfigurieren von Benutzergruppen.** Benutzergruppen kommen im Zusammenhang mit Authentifizierung und Autorisierung zum Einsatz. Wenn die Benutzer ihre Verbindungen beispielsweise über LDAP herstellen, legen Sie einen LDAP-Autorisierungsbereich an und erstellen Sie dann eine Gruppe. Die Namen der Benutzergruppen müssen mit den Namen dieser Gruppen auf dem LDAP-Server übereinstimmen. Darüber hinaus können Sie lokale Benutzer zur lokalen Authentifizierung auf dem Access Gateway anlegen. Die lokalen Benutzer werden dann Benutzergruppen hinzugefügt. Weitere Informationen zum Konfigurieren lokaler Benutzer finden Sie unter "Konfigurieren lokaler Benutzer" auf Seite 79.
- **Schritt 4: Konfigurieren des Netzwerkzugriffs für Gruppen.** Konfigurieren Sie den Netzwerkzugriff für die erstellten Benutzergruppen. Hierzu gehören die Netzwerkressourcen, auf die die Benutzer in der Gruppe zugreifen können, außerdem die Anwendungsrichtlinien und die Endpunktrichtlinien.

Weitere Informationen zum Konfigurieren von zugänglichen Netzwerken, Benutzergruppen und Netzwerkzugriff für Benutzer finden Sie unter "Konfigurieren von Netzwerkzugriff und Gruppenressourcen" auf Seite 111.

Citrix empfiehlt, sich mit den Szenarien unter "Beispiele für die Konfiguration des Netzwerkzugriffs" auf Seite 241 vertraut zu machen, bevor Sie den Netzwerkzugriff für das Gerät konfigurieren.

KAPITEL 6

Konfigurieren der Authentifizierung und Autorisierung

Das Access Gateway unterstützt verschiedene Authentifizierungstypen für die Authentifizierung der Benutzer. Sie können Authentifizierungsbereiche (authentication realms) auf dem Access Gateway konfigurieren, die die Einstellungen für den Authentifizierungstyp enthalten. Der Bereich "Default" ist automatisch für die lokale Authentifizierung konfiguriert. Sie können ihn anpassen, sodass andere Authentifizierungstypen unterstützt werden.

Außerdem können Sie Autorisierungstypen für Benutzer konfigurieren. Dazu gehören lokale, NTLM-, LDAP- und RADIUS-Autorisierung.

Dieses Kapitel enthält:

- "Voraussetzungen für die Authentifizierung auf dem Access Gateway"
- "Konfigurieren der Authentifizierung auf dem Access Gateway"
- "Konfigurieren des Bereichs "Default""
- "Konfigurieren der lokalen Authentifizierung"
- "Konfigurieren lokaler Benutzer"
- "Konfigurieren von LDAP-Authentifizierung und -Autorisierung"
- "Konfigurieren von RADIUS-Authentifizierung und -Autorisierung"
- "Konfigurieren der RSA SecurID-Authentifizierung"
- "Konfigurieren der Authentifizierung mit Secure Computing SafeWord"
- "Konfigurieren der Gemalto Protiva-Authentifizierung"
- "Konfigurieren von NTLM-Authentifizierung und -Autorisierung"
- "Konfigurieren von erweiterten Optionen für die Authentifizierung"
- "Konfigurieren von Zweimethodenauthentifizierung"
- "Ändern der Beschriftung von Kennwortfeldern"

Voraussetzungen für die Authentifizierung auf dem Access Gateway

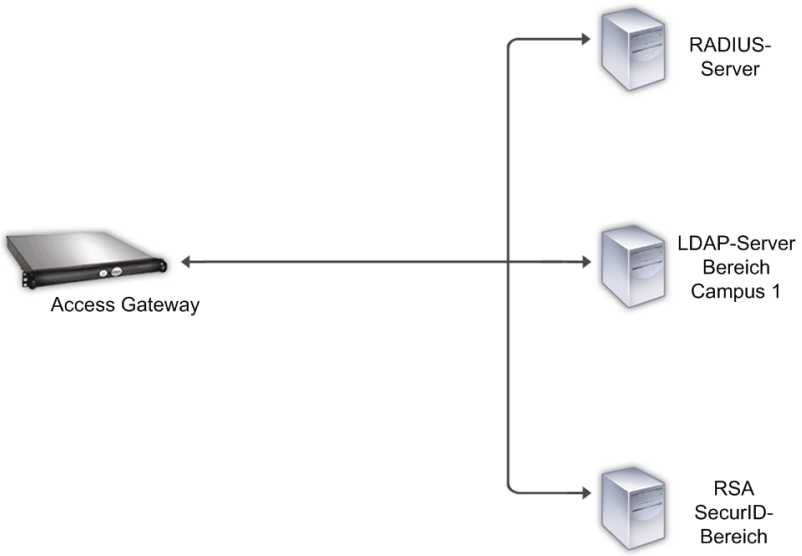
Wenn für die Gruppe des Benutzers keine dieser Authentifizierungsmethoden konfiguriert ist, erfolgt die Authentifizierung anhand der lokalen Benutzerauthentifizierungsdatenbank des Access Gateways. Die Authentifizierung wird in den folgenden Fällen auf dem Access Gateway konfiguriert:

- Das Access Gateway wird in der DMZ oder im sicheren Netzwerk bereitgestellt und die Benutzer stellen eine direkte Verbindung zum Gerät her.
- Das Access Gateway wird in der DMZ bereitgestellt und das Webinterface ist ebenfalls in der DMZ hinter dem Access Gateway.
- Das Access Gateway wird in der DMZ und das Webinterface im sicheren Netzwerk bereitgestellt.

Wenn das Webinterface parallel zum Access Gateway verwendet wird oder das Gerät zur Verwendung von Citrix XenApp Plug-ins konfiguriert ist und das Webinterface Verbindungen zu veröffentlichten Anwendungen in einer Serverfarm herstellt, besteht die Möglichkeit, die Autorisierung auf dem Access Gateway zu konfigurieren.

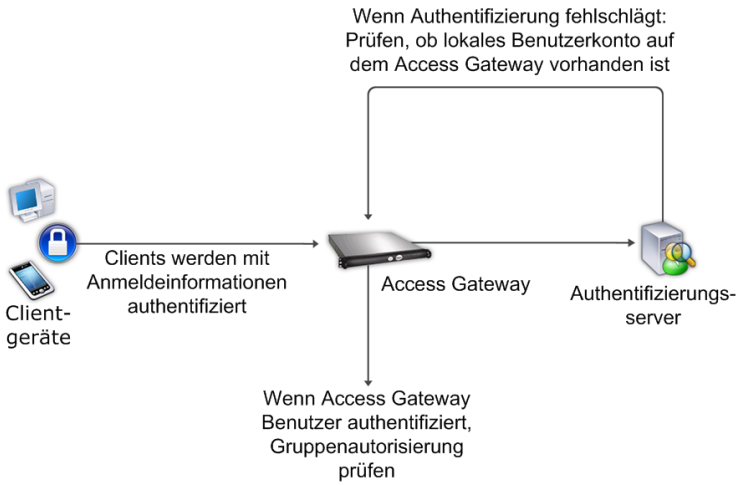
Konfigurieren der Authentifizierung auf dem Access Gateway

Standardmäßig authentifiziert das Access Gateway die Benutzer anhand einer lokal im Access Gateway gespeicherten Benutzerliste. Sie können das Access Gateway für die Verwendung von LDAP-, RADIUS-, RSA SecurID-, Secure Computing SafeWord-, Gemalto Protiva- oder NTLM (Windows NT 4.0)-Authentifizierungsservern konfigurieren. Das Access Gateway unterstützt die bereichsbasierte Authentifizierung, sodass auch Sites mit mehr als einem LDAP- oder RADIUS-Server oder mit einer Kombination von Authentifizierungsservern unterstützt werden.



Kommunikation zwischen Access Gateway und Authentifizierungsservern

Ist ein Benutzer nicht auf dem Authentifizierungsserver oder schlägt die Authentifizierung auf diesem Server fehl, versucht das Access Gateway, den Benutzer anhand der lokalen Benutzerliste zu authentifizieren, wenn auf der Registerkarte **Authentication > Settings** das Kontrollkästchen **Use the local user database on the Access Gateway** aktiviert ist.



Kommunikation zwischen dem Clientgerät, dem Access Gateway und dem lokalen Benutzerkonto bei Fehlschlagen der Authentifizierung auf dem Authentifizierungsserver

Nach der Authentifizierung eines Benutzers führt das Access Gateway eine Gruppenautorisierung durch. Dazu werden die Informationen der Gruppe des Benutzers von einem LDAP-Server, einem RADIUS-Server, einem Windows NT 4.0-Server (zur NTLM-Autorisierung) oder der lokalen Gruppendatei (sofern nicht auf dem LDAP- oder RADIUS-Server verfügbar) abgerufen. Wenn für den Benutzer Gruppeninformationen verfügbar sind, überprüft das Access Gateway anschließend die für die Gruppe zulässigen Netzwerkressourcen. Die LDAP-Autorisierung kann mit allen unterstützten Authentifizierungsmethoden verwendet werden.

Die vom LDAP-Server abgerufenen Gruppennamen werden mit den Gruppennamen verglichen, die lokal im Access Gateway erstellt wurden. Wenn die Gruppennamen übereinstimmen, werden die Eigenschaften der lokalen Gruppe auf die Gruppe angewendet, die von den LDAP-Servern abgerufen wurde.

Konfigurieren der Authentifizierung ohne Autorisierung

Das Access Gateway kann so konfiguriert werden, dass Benutzer authentifiziert werden, ohne dass eine Autorisierung erforderlich ist. Wenn ein Benutzer nicht autorisiert ist, führt das Access Gateway keine Gruppenautorisierung durch. Dem Benutzer werden die Einstellungen der Standardbenutzergruppe zugewiesen.

So stellen Sie auf dem Access Gateway ein, dass keine Autorisierung erforderlich ist

1. Öffnen Sie auf der Registerkarte **Authentication** einen Authentifizierungsbereich
2. Klicken Sie auf die Registerkarte **Authorization** und wählen Sie unter **Authorization type** die Option **No authorization** und klicken Sie auf **Submit**.

Konfigurieren des Bereichs "Default"

Das Access Gateway verfügt über einen permanenten Bereich mit der Bezeichnung Default. Der Bereich "Default" ist für lokale Authentifizierung vorkonfiguriert. Wenn Sie die Authentifizierungsmethode des Bereichs "Default" ändern möchten, muss dieser gelöscht sofort durch einen neuen Bereich "Default" ersetzt werden.

Der Bereich "Default" wird verwendet, wenn ein Benutzer bei der Anmeldung am Access Gateway lediglich einen Benutzernamen eingibt. Bei allen anderen Bereichen muss beim Anmelden ein Bereichsname eingegeben werden. Wenn sich die meisten Benutzer bei einem nicht-lokalen Authentifizierungsbereich anmelden, sollten Sie daher den Authentifizierungstyp für den Bereich "Default" ändern.

Entfernen Sie zum Ändern des Authentifizierungstyps des Bereichs "Default" diesen Bereich und erstellen Sie dann sofort einen neuen mit der entsprechenden Authentifizierungskonfiguration.

Hinweis: Wird der gelöschte Bereich "Default" nicht sofort durch einen neuen ersetzt, wird der Originalbereich automatisch wiederhergestellt.

So können Sie den Bereich "Default" entfernen und neu erstellen

1. Klicken Sie auf die Registerkarte **Authentication**.
2. Öffnen Sie das Fenster für den Bereich "Default".
3. Wählen Sie im Menü **Action** den Befehl **Remove Default realm**.

   Es wird eine Warnmeldung angezeigt. Klicken Sie auf **Ja**.
4. Geben Sie unter **Add an Authentication Realm** in das Feld **Realm name** "Default" ein.

   Wichtig: Beim Erstellen eines neuen Bereichs muss beim Wort "Default" die Groß- und Kleinschreibung beachtet und ein großes "D" verwendet werden.

   ---
5. Tun Sie Folgendes:
   - Wenn Sie einen einzelnen Authentifizierungstyp konfigurieren, wählen Sie **One Source** aus und klicken Sie auf **Add**.
   - Wenn Sie Zweimethodenauthentifizierung konfigurieren, wählen Sie **Two Source** aus und klicken Sie auf **Add**.

6. Wählen Sie unter **Authentication type** den Authentifizierungstyp aus und klicken Sie dann auf **OK**.
7. Konfigurieren Sie die Authentifizierungseinstellungen. Weitere Informationen finden Sie in den folgenden Abschnitten:
    - "Konfigurieren der lokalen Authentifizierung" auf Seite 78
    - "Konfigurieren von LDAP-Authentifizierung und -Autorisierung" auf Seite 81
    - "Konfigurieren von RADIUS-Authentifizierung und -Autorisierung" auf Seite 90
    - "Konfigurieren der RSA SecurID-Authentifizierung" auf Seite 95
    - "Konfigurieren der Authentifizierung mit Secure Computing SafeWord" auf Seite 99
    - "Konfigurieren der Gemalto Protiva-Authentifizierung" auf Seite 102
    - "Konfigurieren von NTLM-Authentifizierung und -Autorisierung" auf Seite 103

Erstellen von zusätzlichen Bereichen

Neben dem Bereich "Default" können noch weitere Bereiche erstellt werden. Beispiel: Der Bereich "Default" soll für die Authentifizierung bei einem LDAP-Server verwendet werden. Wenn Sie für die Benutzer zusätzliche Authentifizierungsmethoden verwenden möchten, wie z. B. RADIUS, SafeWord, RSA SecurID, NTLM oder lokale Authentifizierung am Gerät, können Sie für jede dieser Methoden einen Bereich erstellen. Wenn sich ein Benutzer an anderen Bereichen als dem Bereich "Default" anmeldet, muss er den Namen des Bereichs und seinen Benutzernamen eingeben, z. B. *Bereichsname\Benutzername*.

Hinweis: Citrix empfiehlt, die Bereiche nach den dazugehörigen Domänen zu benennen. Dadurch können sich Benutzer entweder mit *Bereichsname\Benutzername* oder mit *Benutzername@Bereichsname* anmelden.

So erstellen Sie einen Bereich

1. Geben Sie auf der Registerkarte **Authentication** unter **Add an Authentication Realm** in das Feld **Realm name** den Namen des Bereichs ein.
2. Tun Sie Folgendes:

   Wenn die Benutzer nur einen Authentifizierungstyp verwenden, klicken Sie auf **One Source**.

   - Oder -

   Wenn die Benutzer zwei Authentifizierungstypen verwenden, klicken Sie auf **Two Source**.
3. Klicken Sie auf **Add**.
4. Wählen Sie unter **Authentication type** die Authentifizierungsmethode aus und klicken Sie auf **OK**.

   Wenn Sie Zweimethodenauthentifizierung konfigurieren, wählen Sie unter **Primary authentication type** den Typ aus, mit dem sich Benutzer zuerst anmelden. Wählen Sie unter **Secondary authentication type** den Typ aus, mit dem sich die Benutzer als zweites anmelden. Weitere Informationen hierzu finden Sie unter "Konfigurieren von Zweimethodenauthentifizierung" auf Seite 108.
5. Konfigurieren Sie die Einstellungen für den Bereich und klicken Sie dann auf **Submit**.

Konfigurieren von Single Sign-On beim Webinterface

Wenn Sie Single Sign-On für das Webinterface konfigurieren, müssen Sie den Bereich "Default" für die Authentifizierung verwenden. Wenn Sie einen anderen Bereich für das Single Sign-On am Webinterface verwenden, können Benutzer sich nicht anmelden.

Weitere Informationen finden Sie in der *Citrix Access Gateway Standard Edition – Integrationsdokumentation für Citrix XenApp und Citrix XenDesktop*.

Entfernen von Bereichen

Wenn Sie einen Authentifizierungsserver außer Betrieb nehmen oder einen Domänenserver entfernen, können Sie jeden Bereich mit Ausnahme des Bereichs "Default" entfernen. Den Bereich "Default" können Sie nur entfernen, wenn Sie sofort wieder einen neuen Bereich mit diesem Namen erstellen. Weitere Informationen hierzu finden Sie unter "Konfigurieren des Bereichs "Default"" auf Seite 75.

So entfernen Sie einen Bereich

1. Öffnen Sie auf der Registerkarte **Authentication** den Bereich, der entfernt werden soll.
2. Klicken Sie im Menü **Action** auf **Remove *Bereichsname* realm**.

   Der Bereich wird entfernt.

Konfigurieren der lokalen Authentifizierung

Bei einer Neuinstallation wird für den Bereich "Default" die lokale Authentifizierung festgelegt. Auf diese Weise können sich die Benutzer am Access Gateway anmelden, ohne einen Bereichsnamen eingeben zu müssen.

Wenn einige Benutzer sich ausschließlich anhand der lokalen Benutzerliste des Access Gateways authentifizieren, können Sie für den Bereich "Default" die lokale Authentifizierung beibehalten. Sie können alternativ dazu auch einen neuen Bereich für die lokale Authentifizierung erstellen und den Bereich "Default" dann für einen anderen Authentifizierungstyp verwenden.

Wenn sich alle Benutzer unter Verwendung von Authentifizierungsservern authentifizieren, wird kein Bereich für die lokale Authentifizierung benötigt. Das Access Gateway kann die lokale Benutzerdatenbank auf dem Gerät nach Authentifizierungsinformationen überprüfen, wenn die Authentifizierung eines Benutzers auf einem anderen Authentifizierungsserver fehlschlägt. Wenn Sie z. B. LDAP verwenden und die Authentifizierung fehlschlägt, können sich die Benutzer mit der lokalen Benutzerdatenbank anmelden.

So stellen Sie die Authentifizierung mit der lokalen Benutzerliste auf dem Access Gateway ein

1. Öffnen Sie auf der Registerkarte **Authentication** den Authentifizierungsbereich, in dem Sie lokale Authentifizierung konfigurieren möchten.
2. Klicken Sie auf die Registerkarte **Settings**.
3. Klicken Sie auf **Use the local user database on the Access Gateway** und dann auf **Submit**.

Hinweis: Dieses Kontrollkästchen steht nicht zur Verfügung, wenn der Bereich für lokale Authentifizierung konfiguriert ist.

Konfigurieren lokaler Benutzer

Sie können auf dem Access Gateway lokale Benutzerkonten erstellen und so die Liste der Benutzer auf den Authentifizierungsservern ergänzen. So können Sie beispielsweise lokale Benutzerkonten für temporäre Benutzer, wie z. B. Unternehmensberater oder Besucher, erstellen, ohne auf dem Authentifizierungsserver einen Eintrag für diese Benutzer erstellen zu müssen. In diesem Fall fügen Sie den Benutzer der lokalen Benutzerliste des Access Gateways hinzu.

Wenn Sie Benutzer einer anderen Gruppe hinzufügen möchten, klicken Sie unter **Local Users** auf den jeweiligen Benutzer und ziehen Sie ihn auf die entsprechende Benutzergruppe.

Wenn Benutzer keiner der von Ihnen auf dem Access Gateway definierten Gruppen angehören, werden ihnen die Einstellungen der Standardbenutzergruppe zugewiesen. Wenn Benutzer einer anderen Gruppe als der Standardgruppe angehören, werden ihnen nur dann die Einstellungen der Standardgruppe zugewiesen, wenn die Gruppe zur Übernahme dieser Einstellungen konfiguriert wurde. Weitere Informationen hierzu finden Sie unter "Eigenschaften der Standardgruppe ("Default")" auf Seite 119.

So erstellen Sie Benutzer auf dem Access Gateway

1. Klicken Sie auf die **Registerkarte** Access Policy Manager.
2. Klicken Sie mit der rechten Maustaste im linken Bereich auf **Local Users** und klicken Sie dann auf **New User**.
3. Geben Sie unter **User Name** einen Benutzernamen ein. Benutzernamen können Leerzeichen enthalten.

   Hinweis: Bei Benutzernamen muss die Groß- und Kleinschreibung nicht beachtet werden. Verwenden Sie keinen Schrägstrich (/) oder Klammeraffen (@) im Benutzernamen oder im Kennwort. Kennwörter dürfen nicht mit einem Leerzeichen beginnen oder enden.

4. Geben Sie in die Felder **Password** und **Verify Password** das Kennwort für den Benutzer ein und klicken Sie auf **OK**.

   Dieses Kennwort müssen Benutzer bei der Anmeldung eingeben. Kennwörter müssen zwischen 6 und 127 Zeichen lang sein.

So löschen Sie einen Benutzer vom Access Gateway

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Klicken Sie im linken Bereich in der Liste **Local Users** mit der rechten Maustaste auf den entsprechenden Benutzer und klicken Sie dann auf **Remove**.

Zuweisen von Benutzern zu mehreren Gruppen

Nachdem Sie die lokale Benutzerliste erstellt haben, können Sie die Benutzer den auf dem Access Gateway erstellten Gruppen hinzufügen.

Wenn Sie mehrere Gruppen mit einem Benutzerkonto verknüpfen, werden für den Benutzer die Eigenschaften der ersten auf der Registerkarte **Group Priority** ausgewählten Gruppe verwendet.

So fügen Sie einen Benutzer einer Gruppe hinzu

Klicken Sie in der Liste **Local Users** auf den Benutzer und ziehen Sie ihn auf eine Gruppe.

Ändern von Kennwörtern für Benutzer

Im Administration Tool können Sie das Kennwort eines Benutzers ändern.

So ändern Sie das Kennwort eines Benutzers

1. Klicken Sie auf der Registerkarte **Access Policy Manager** mit der rechten Maustaste auf einen Benutzer und klicken Sie dann auf **Set Password**.
2. Geben Sie das Kennwort zweimal ein und klicken Sie dann auf **OK**.

Konfigurieren von LDAP-Authentifizierung und -Autorisierung

Sie können das Access Gateway für die Authentifizierung des Benutzerzugriffs mit einem oder mehreren LDAP-Servern konfigurieren. Ist ein Benutzer nicht in einem LDAP-Verzeichnis oder schlägt die Authentifizierung bei einem Server fehl, überprüft das Access Gateway die Anmeldeinformationen des Benutzers anhand der lokal im Access Gateway gespeicherten Benutzerinformationen.

Für die LDAP-Autorisierung müssen die Gruppennamen in Active Directory, auf dem LDAP-Server und auf dem Access Gateway übereinstimmen (inklusive Leerzeichen und Groß-/Kleinschreibung).

Die LDAP-Authentifizierung wird standardmäßig mit SSL/TLS gesichert. Es gibt zwei Arten sicherer LDAP-Verbindungen. Bei der ersten Art nimmt der LDAP-Server die SSL/TLS-Verbindung auf einem Port an, der sich von dem Port unterscheidet, der die unverschlüsselten LDAP-Verbindungen annimmt. Wenn Benutzer die SSL/TLS-Verbindung herstellen, kann der LDAP-Verkehr über diese Verbindung gesendet werden. Bei der zweiten Art sind sowohl unsichere als auch sichere LDAP-Verbindungen zulässig, wobei die Verbindungen alle über denselben Serverport laufen. In diesem Fall muss der Client zum Herstellen einer sicheren Verbindung zunächst eine unverschlüsselte LDAP-Verbindung einrichten. Anschließend wird über diese Verbindung der LDAP-Befehl StartTLS an den Server gesendet. Wenn der LDAP-Server StartTLS unterstützt, wird die Verbindung in eine sichere LDAP-Verbindung mit TLS umgewandelt.

Für LDAP-Verbindungen werden die folgenden Portnummern verwendet:

- 389 für unsichere LDAP-Verbindungen
- 636 für sichere LDAP-Verbindungen
- 3268 für unsichere LDAP-Verbindungen unter Microsoft
- 3269 für sichere LDAP-Verbindungen unter Microsoft

LDAP-Verbindungen, die den Befehl StartTLS verwenden, nutzen die Portnummer 389. Wenn die Portnummern 389 oder 3268 auf dem Access Gateway konfiguriert sind, wird versucht, die Verbindung mit StartTLS herzustellen. Bei Verwendung einer anderen Portnummer erfolgen die Verbindungsversuche mittels SSL/TLS. Können StartTLS oder SSL/TLS nicht verwendet werden, kann die Verbindung nicht hergestellt werden.

Hinweis: Wenn das Access Gateway jedoch neu installiert wurde oder wenn Sie einen neuen LDAP-Bereich erstellen, sind die LDAP-Verbindungen standardmäßig sicher.

Beim Konfigurieren des LDAP-Servers muss die Groß- und Kleinschreibung mit der Schreibung auf dem Server und auf dem Access Gateway identisch sein. Wenn das Stammverzeichnis des LDAP-Servers festgelegt wird, wird auch in allen Unterverzeichnissen nach dem Benutzerattribut gesucht. In großen Verzeichnissen kann sich dies negativ auf die Arbeitsgeschwindigkeit auswirken. Citrix empfiehlt daher die Verwendung einer spezifischen Organisationseinheit.

Die folgende Tabelle enthält Beispiele für Benutzerattributfelder für LDAP-Server:

LDAP-Server	**Benutzerattribut**	**Groß-/ Kleinschreibung relevant**
Microsoft Active Directory-Server	sAMAccountName	Nein
Novell eDirectory	cn	Ja
IBM Directory Server	uid	Ja
Lotus Domino	CN	Ja
Sun ONE-Verzeichnis (früher iPlanet)	uid oder cn	Ja

Die folgende Tabelle enthält Beispiele für den Basis-DN:

LDAP-Server	**Basis-DN**
Microsoft Active Directory-Server	DC=citrix, DC=local
Novell eDirectory	dc=citrix,dc=net
IBM Directory Server	cn=users
Lotus Domino	OU=City, O=Citrix, C=US
Sun ONE-Verzeichnis (früher iPlanet)	ou=People,dc=citrix,dc=com

Die folgende Tabelle enthält Beispiele für den Bind-DN:

LDAP-Server	Bind-DN
Microsoft Active Directory-Server	CN=Administrator, CN=Users, DC=citrix, DC=local
Novell eDirectory	cn=admin, dc=citrix, dc=net
IBM Directory Server	LDAP_dn
Lotus Domino	CN=Notes Administrator, O=Citrix, C=US
Sun ONE-Verzeichnis (früher iPlanet)	uid=admin,ou=Administrators, ou=TopologyManagement,o=NetscapeRoot

Hinweis: Weitere Informationen zu LDAP-Servereinstellungen finden Sie unter "Bestimmen der Attribute in Ihrem LDAP-Verzeichnis" auf Seite 89.

So erstellen Sie einen LDAP-Authentifizierungsbereich

1. Klicken Sie auf die Registerkarte **Authentication**.
2. Geben Sie unter **Add an Authentication Realm** in das Feld **Realm name** einen Namen für den Authentifizierungsbereich ein.

   Wenn Ihre Site mehrere Authentifizierungsbereiche besitzt, sollten Sie einen Namen verwenden, aus dem deutlich der LDAP-Bereich hervorgeht, für den Sie die Einstellungen festlegen. Bei Bereichsnamen ist auf die Groß- und Kleinschreibung zu achten. Darüber hinaus können sie Leerzeichen enthalten.

   Hinweis: Wenn der Bereich "Default" die LDAP-Authentifizierung verwenden soll, entfernen Sie den Bereich "Default" wie unter "So können Sie den Bereich "Default" entfernen und neu erstellen" auf Seite 75 beschrieben.

3. Wählen Sie **One Source** und klicken Sie auf **Add**.
4. Wählen Sie im Dialogfeld **Select Authentication Type** unter **Authentication Type** die Option **LDAP authentication** und klicken Sie auf **OK**.

   Das Dialogfeld **Realm** mit dem Namen des Bereichs wird geöffnet.

Konfigurieren Sie nach der Erstellung des Bereichs die LDAP-Authentifizierung.

So konfigurieren Sie die LDAP-Authentifizierung

1. Geben Sie unter **IP Address or FQDN** die IP- oder Webadresse des LDAP-Servers ein.
2. Geben Sie im Feld **Port** die Portnummer ein.

   Die Standardeinstellung für den LDAP-Serverport ist 389. Wenn Sie eine indexierte Datenbank verwenden, wie z. B. Microsoft Active Directory mit einem globalen Katalog, können Sie durch Ändern des LDAP-Serverports zu 3268 die Geschwindigkeit der LDAP-Abfragen deutlich erhöhen.

   Wenn Ihr Verzeichnis nicht indexiert ist, empfiehlt Citrix anstelle einer anonymen Verbindung zwischen dem Access Gateway und der Datenbank die Verwendung einer administrativen Verbindung. Die Verwendung einer solchen Verbindung verbessert die Downloadgeschwindigkeit.
3. Tun Sie Folgendes:

   - Um unsichere LDAP-Verbindungen zuzulassen, aktivieren Sie die Option **Allow unsecure connection**.
   - Um LDAP-Verbindungen zu sichern, deaktivieren Sie die Option **Allow unsecure connection**.

     Wenn diese Option nicht aktiviert ist, sind alle LDAP-Verbindungen sicher.
4. Geben Sie unter **Administrator bind DN** den Administrator-Bind-DN für Abfragen ein, die an Ihr LDAP-Verzeichnis gerichtet sind.

   Beispielsyntax für Bind-DN:
   domäne/benutzername
   ou=administrator,dc=ace,dc=com
   benutzer@domäne.name" (für Active Directory)
   cn=Administrator,cn=Benutzer,dc=ace,dc=com

   Für Active Directory muss der Gruppenname wie folgt angegeben werden: cn=*Gruppenname*. Der auf dem Access Gateway definierte Gruppenname muss identisch mit dem auf dem LDAP-Server definierten Gruppennamen sein.

   Bei anderen LDAP-Verzeichnissen ist der Gruppenname entweder nicht erforderlich oder er muss, sofern er doch nötig ist, in folgender Form angegeben werden: "ou=*Gruppenname*".

   Das Access Gateway registriert sich mit den Administratoranmeldeinformationen beim LDAP-Server und sucht dann nach dem Benutzer. Wenn der Benutzer gefunden ist, hebt das Access Gateway die Registrierung mit den Administratoranmeldeinformationen auf und registriert sich mit den Benutzeranmeldeinformationen neu.

5. Geben Sie unter **Administrator password** das Kennwort ein.
6. Geben Sie unter **Base DN (location of users)** den Basis-DN für die Benutzer ein.

   Der Basis-DN wird normalerweise vom Bind-DN abgeleitet, indem der Benutzername entfernt und die Gruppe angegeben wird, in der sich die Benutzer befinden. Beispielsyntax für Basis-DN:
   ou=benutzer,dc=ace,dc=com
   cn=Benutzer,dc=ace,dc=com
7. Geben Sie unter **Server logon name attribute** das Attribut ein, unter dem das Access Gateway nach den Benutzeranmeldenamen für den LDAP-Server suchen soll, den Sie gerade konfigurieren. Das Standardattribut ist sAMAccountName. Wenn Sie andere Verzeichnisse verwenden, verwenden Sie als Attribut **cn**. Klicken Sie auf **Submit**.

Das Access Gateway kann so konfiguriert werden, dass der Benutzerzugriff mit einem oder mehreren LDAP-Server(n) authentifiziert wird. Ist ein Benutzer nicht in einem LDAP-Verzeichnis oder schlägt die Authentifizierung auf einem Server fehl, überprüft das Access Gateway den Benutzer anhand der lokal auf dem Access Gateway gespeicherten Benutzerinformationen, sofern auf der Registerkarte **Settings** die Option **Use the local user database on the Access Gateway** aktiviert ist.

Für die LDAP-Autorisierung müssen die Gruppennamen in Active Directory, auf dem Access Gateway und auf dem LDAP-Server identisch sein (inklusive Leerzeichen und Groß-/Kleinschreibung).

Hinweis: Weitere Informationen zur Festlegung der LDAP-Servereinstellungen finden Sie unter "Bestimmen der Attribute in Ihrem LDAP-Verzeichnis" auf Seite 89.

Konfigurieren der LDAP-Autorisierung

Im Folgenden werden die LDAP-Gruppenmitgliedschaftsattribute beschrieben, die mit der Access Gateway-Autorisierung funktionieren und nicht funktionieren.

Für die LDAP-Authentifizierung können Sie die folgenden Autorisierungstypen verwenden:

- Lokale Autorisierung
- LDAP-Autorisierung
- Keine Autorisierung

Wenn Sie die Zweimethodenauthentifizierung verwenden, basiert die Autorisierung auf der primären, nicht der sekundären Authentifizierungsmethode.

Hinweis: Wenn Sie die gleichen Benutzer der lokalen Gruppe auf dem Access Gateway und einer LDAP- oder Active Directory-Gruppe hinzugefügt haben, verwendet Access Gateway die Eigenschaften beider Gruppen für die Autorisierung. Der verwendete Autorisierungstyp ist von der Gruppenpriorität abhängig.

Auswertung der Gruppenmitgliedschaft anhand von Gruppenobjekten

Einige LDAP-Server, die die Gruppenmitgliedschaft indirekt anhand von Gruppenobjekten auswerten, können die Access Gateway-Autorisierung verwenden.

Es gibt LDAP-Server, bei denen die Benutzerobjekte Informationen zu den Gruppen enthalten können, zu denen sie gehören. Dazu gehören z. B. Active Directory und eDirectory. Die Gruppenmitgliedschaft eines Benutzers kann aus berechenbaren Attributen aus dem Benutzerobjekt hervorgehen, wie das z. B. beim IBM Directory Server oder beim Sun ONE-Verzeichnisserver der Fall ist. Bei einigen LDAP-Servern kann dieses Attribut verwendet werden, um die dynamische Gruppenmitgliedschaft, die verschachtelte Gruppenmitgliedschaft und die statische Gruppenmitgliedschaft eines Benutzers einzuschließen, sodass alle Gruppenmitgliedschaften anhand eines einzelnen Attributs gefunden werden können.

So können z. B. in IBM Directory Server alle Gruppenmitgliedschaften (in statischen, dynamischen und verschachtelten Gruppen) über das Attribut ibm-allGroups zurückgegeben werden. In Sun ONE werden alle Rollen, einschließlich der verwalteten, gefilterten und verschachtelten Rollen, mit dem Attribut nsRole berechnet.

Auswertung der Gruppenmitgliedschaft anhand von Gruppenobjekten ohne Access Gateway-Autorisierung

Einige LDAP-Server, die die Gruppenmitgliedschaft indirekt anhand von Gruppenobjekten auswerten, verwenden die Access Gateway-Autorisierung nicht.

Es gibt LDAP-Server, bei denen nur Gruppenobjekte Informationen über Benutzer enthalten können (z. B. der Lotus Domino-LDAP-Server). Das Benutzerobjekt darf bei diesen LDAP-Servern keine Informationen über Gruppen enthalten. Bei solchen LDAP-Servern erfolgt die Suche nach der Gruppenmitgliedschaft, indem der Benutzer in der Mitgliederliste der Gruppen gesucht wird.

Gruppenattributfelder für die LDAP-Autorisierung

Die folgende Tabelle enthält Beispiele für LDAP-Gruppenattributfelder.

Microsoft Active Directory-Server	memberOf
Novell eDirectory	groupMembership
IBM Directory Server	ibm-allGroups
Sun ONE-Verzeichnis (früher iPlanet)	nsRole

So konfigurieren Sie die LDAP-Autorisierung

1. Klicken Sie auf die Registerkarte **Authorization**.
2. Wählen Sie unter **Authorization type** die Option **LDAP authorization**.
3. Geben Sie unter **IP address or FQDN** die IP- oder Webadresse des LDAP-Servers ein.
4. Geben Sie im Feld **Port** die Portnummer ein. Der Standardport ist 389.
5. Tun Sie Folgendes:
   - Um unsichere LDAP-Verbindungen zuzulassen, aktivieren Sie die Option **Allow unsecure connection**.
   - Um LDAP-Verbindungen zu sichern, deaktivieren Sie die Option **Allow unsecure connection**.

     Wenn diese Option nicht aktiviert ist, sind alle LDAP-Verbindungen sicher.

6. Geben Sie unter **Administrator bind DN** den Administrator-Bind-DN für Abfragen ein, die an Ihr LDAP-Verzeichnis gerichtet sind.

   Beispielsyntax für Bind-DN:
   domäne/benutzername"
   ou=administrator,dc=ace,dc=com"
   "benutzer@domäne.name" (für Active Directory)
   "cn=Administrator,cn=Benutzer,dc=ace,dc=com"

   Für Active Directory muss der Gruppenname wie folgt angegeben werden: cn=*Gruppenname*. Der auf dem Access Gateway definierte Gruppenname muss identisch mit dem auf dem LDAP-Server definierten Gruppennamen sein.

   Bei anderen LDAP-Verzeichnissen ist der Gruppenname entweder nicht erforderlich oder er muss, sofern er doch nötig ist, in folgender Form angegeben werden: ou=*Gruppenname*.

   Das Access Gateway registriert sich mit den Administratoranmeldeinformationen beim LDAP-Server und sucht dann nach dem Benutzer. Wenn der Benutzer gefunden ist, hebt das Access Gateway die Registrierung mit den Administratoranmeldeinformationen auf und registriert sich mit den Benutzeranmeldeinformationen erneut.

7. Geben Sie unter **Administrator password** das Kennwort ein.

8. Geben Sie unter **Base DN (location of users)** den Basis-DN für die Benutzer ein.

   Der Basis-DN wird normalerweise vom Bind-DN abgeleitet, indem der Benutzername entfernt und die Gruppe angegeben wird, in der sich die Benutzer befinden. Beispielsyntax für Bind-DN:
   "ou=Benutzer,dc=ace,dc=com"
   "cn=Benutzer,dc=ace,dc=com"

9. Geben Sie unter **Server logon name attribute** das Attribut ein, unter dem das Access Gateway nach den Benutzeranmeldenamen für den LDAP-Server suchen soll, den Sie gerade konfigurieren. Das Standardattribut ist cn. Bei Verwendung von Active Directory ist das Attribut cn einzugeben.

10. Geben Sie unter **Group attribute** den Namen des Attributs ein. Standard ist "memberOf". Mit diesem Attribut kann das Access Gateway bei der Autorisierung die Gruppen abrufen, bei denen der Benutzer Mitglied ist. Klicken Sie auf **Submit**.

Verwenden von Zertifikaten für sichere LDAP-Verbindungen

Für die LDAP-Authentifizierung und -Autorisierung können Sie ein sicheres Clientzertifikat verwenden. Hierfür benötigen Sie eine Zertifizierungsstelle im Unternehmen, z. B. die Zertifikatdienste in Windows Server 2003, die auf demselben Computer wie Active Directory ausgeführt werden. Über die Zertifizierungsstelle können Sie ein Clientzertifikat erstellen.

Für die LDAP-Authentifizierung und -Autorisierung muss das Clientzertifikat sicher sein und SSL verwenden. Sichere Clientzertifikate für LDAP werden auf das Access Gateway hochgeladen.

So laden Sie ein sicheres Clientzertifikat für LDAP hoch

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Access Gateway und klicken Sie auf die Registerkarte **Administration**.
2. Klicken Sie neben **Upload a .pem private key and signed certificate** auf **Browse**.
3. Gehen Sie zum Clientzertifikat und klicken Sie auf **Öffnen**.

Bestimmen der Attribute in Ihrem LDAP-Verzeichnis

Wenn Sie bei der Bestimmung Ihrer LDAP-Verzeichnisattribute Hilfe benötigen, können Sie mit der kostenlos erhältlichen Anwendung LDAP Browser von Softerra ganz einfach nach diesen Attributen suchen.

Laden Sie die kostenlos erhältliche Anwendung LDAP Browser von der Softerra LDAP Administrator-Website (http://www.ldapbrowser.com) herunter. Die Anwendung ist auch mit deutscher Benutzeroberfläche erhältlich. Legen Sie nach der Installation des Browsers folgende Attribute fest:

- Hostname oder IP-Adresse Ihres LDAP-Servers.
- Port Ihres LDAP-Servers. Der Standardwert ist 389.
- Das Feld "Base DN" kann leer gelassen werden.

  Anhand der von LDAP Browser bereitgestellten Informationen können Sie den Basis-DN bestimmen, der auf der Registerkarte **Authentication** benötigt wird.

- Mit dem Kontrollkästchen "Anonymous Bind" wird festgelegt, ob der LDAP-Server die Anmeldeinformationen der Benutzer benötigt, um eine Verbindung zum Browser herzustellen. Wenn der LDAP-Server die Anmeldeinformationen benötigt, lassen Sie das Kontrollkästchen deaktiviert.

Wenn alle Einstellungen vorgenommen wurden, zeigt LDAP Browser im linken Bereich den Profilnamen an und stellt eine Verbindung zum LDAP-Server her.

Konfigurieren von RADIUS-Authentifizierung und -Autorisierung

Sie können das Access Gateway für die Authentifizierung des Benutzerzugriffs mit einem oder mehreren RADIUS-Server(n) konfigurieren. Für jeden für die Authentifizierung verwendeten RADIUS-Bereich können Sie einen primären und einen sekundären RADIUS-Server konfigurieren. Wenn der primäre RADIUS-Server nicht verfügbar ist, versucht das Access Gateway, die Authentifizierung für diesen Bereich mit dem sekundären RADIUS-Server vorzunehmen.

Ist ein Benutzer nicht auf den RADIUS-Servern oder schlägt die Authentifizierung fehl, überprüft das Access Gateway den Benutzer anhand der lokal auf dem Access Gateway gespeicherten Benutzerinformationen, sofern auf der Registerkarte **Settings** des Bereichs die Option **Use the local user database on the Access Gateway** aktiviert ist.

Die Access Gateway-Software enthält außerdem die RADIUS-Autorisierung, die mit der RAS-Richtlinie im Microsoft-Internetauthentifizierungsdienst (IAS) konfiguriert wird. Während der Konfiguration des Access Gateways müssen die folgenden Informationen bereitgestellt werden:

- Vendor Code (entspricht dem im IAS eingegebenen Herstellercode).
- Vendor-assigned atttribute number (entspricht der vom Hersteller zugewiesenen Attributnummer).
- Attribute Value Prefix (entspricht dem im IAS definierten Attributwert). Der Standardname ist *CTXSUserGroups*=.
- Das Trennzeichen (Separator) muss angegeben werden, wenn in der RADIUS-Konfiguration mehrere Benutzergruppen enthalten sind. Als Trennzeichen kann ein Leerzeichen, ein Punkt, ein Semikolon oder ein Doppelpunkt verwendet werden.

Wenn IAS nicht auf dem RADIUS-Server installiert ist, können Sie es über die Systemsteuerung installieren. Weitere Informationen finden Sie in der Windows-Onlinehilfe.

Zum Konfigurieren des IAS installieren Sie das Snap-In für IAS über die Microsoft Management Console (MMC). Führen Sie den Installationsassistenten aus und wählen Sie dabei die folgenden Einstellungen:

- Wählen Sie Lokalen Computer.
- Wählen Sie RAS-Richtlinien und erstellen Sie eine benutzerdefinierte Richtlinie.
- Wählen Sie für die Richtlinie Windows-Groups.
- Wählen Sie Verschlüsselte Authentifizierung (CHAP) und Unverschlüsselte Authentifizierung (PAP, SPAP).
- Wählen Sie nicht MS-CHAP v2 und MS-CHAP.
- Wählen Sie als Attributnamen Vendor-Specifc aus.

  Access Gateway benötigt das herstellerspezifische Attribut, um die in der Gruppe auf dem Server definierten Benutzer mit den Benutzern auf dem Access Gateway abzugleichen. Dies erfolgt durch Senden der herstellerspezifischen Attribute an das Access Gateway. Als Hersteller muss RADIUS Standard ausgewählt werden.
- Die RADIUS-Standardeinstellung ist 0. Verwenden Sie diese Zahl als Herstellercode.
- Die vom Hersteller zugewiesene Attributnummer ist 0.

  Dies ist der zugewiesene Wert für das Attribut CTSXUserGroups. Das Attribut hat das Format einer Zeichenfolge.
- Wählen Sie als Attributformat Zeichenfolge aus.

  Geben Sie unter Attributwert den Attributnamen und die Gruppen ein.

  Für das Access Gateway ist der Attributwert: CTXSUserGroups=*Gruppenname*. Wenn zwei Gruppen definiert sind, z. B. die Gruppen "Vertrieb" und "Finanzen", ist der Attributwert CTXSUserGroups=Vertrieb;Finanzen. Die Gruppen sind dabei jeweils durch ein Semikolon zu trennen.
- Entfernen Sie im Dialogfeld **Einwählprofil bearbeiten** alle anderen Einträge außer dem Eintrag Vendor-specific.

Wenn Sie mit dem Konfigurieren der RAS-Richtlinie im IAS fertig sind, gehen Sie zum Access Gateway und konfigurieren Sie die RADIUS-Authentifizierung und -Autorisierung.

So konfigurieren Sie die RADIUS-Authentifizierung

1. Klicken Sie auf die Registerkarte **Authentication**.
2. Geben Sie im Feld **Realm name** einen Namen für den Authentifizierungsbereich ein, wählen Sie **One Source** und klicken Sie dann auf **Add**.

   Hinweis: Wenn der Bereich "Default" RADIUS-Authentifizierung verwenden soll, entfernen Sie den Bereich "Default" wie unter "So können Sie den Bereich "Default" entfernen und neu erstellen" auf Seite 75 beschrieben.

   Besitzt Ihre Site mehrere Authentifizierungsbereiche, verwenden Sie einen Namen, aus dem deutlich hervorgeht, für welchen RADIUS-Bereich Sie die Einstellungen festlegen. Bei Bereichsnamen ist auf die Groß- und Kleinschreibung zu achten. Darüber hinaus können sie Leerzeichen enthalten.
3. Wählen Sie unter **Authentication type** die Option **RADIUS authentication** und klicken Sie auf **OK**.

   Das Dialogfeld für den Authentifizierungsbereich wird geöffnet.
4. Geben Sie unter **IP Address** die IP-Adresse des RADIUS-Servers ein.
5. Geben Sie im Feld **Port** die Portnummer ein. Die Standardportnummer ist 1812.
6. Geben Sie im Feld **Server secret** den geheimen RADIUS-Schlüssel ein.

   Der geheime Serverschlüssel wird auf dem RADIUS-Server und auf dem Access Gateway manuell konfiguriert.

   Wichtig: Achten Sie darauf, dass der geheime Serverschlüssel stark genug ist. Ein geheimer Schlüssel ist stark, wenn er aus mindestens acht Zeichen besteht und sich aus Buchstaben, Ziffern und Symbolen zusammensetzt.

   ---
7. Wenn Sie einen sekundären RADIUS-Server verwenden, geben Sie die IP-Adresse, den Port und den geheimen Schlüssel dieses Servers ein.

Informationen über das Konfigurieren der erweiterten Optionen finden Sie unter "Konfigurieren von erweiterten Optionen für die Authentifizierung" auf Seite 106.

RADIUS-Autorisierung

Für die RADIUS-Authentifizierung können Sie die folgenden Autorisierungstypen verwenden:

- RADIUS-Autorisierung
- Lokale Autorisierung
- LDAP-Autorisierung
- Keine Autorisierung

So konfigurieren Sie RADIUS-Autorisierung

1. Klicken Sie auf die Registerkarte **Authentication** und öffnen Sie den Bereich, für den Sie RADIUS-Autorisierung konfigurieren möchten.
2. Klicken Sie auf die Registerkarte **Authorization** und wählen Sie unter **Authorization type** die Option **RADIUS authorization**.
3. Vervollständigen Sie die Einstellungen mit den im IAS definierten Attributen.
4. Klicken Sie auf **Submit**.

Hinweis: Wenn Sie den Microsoft-Internetauthentifizierungsdienst (IAS) als RADIUS-Server verwenden und beim Senden einer Anforderung an den konfigurierten RADIUS-Server durch das Access Gateway eine Fehlermeldung erhalten, wonach der Benutzername oder das Kennwort ungültig ist, wählen Sie in den IAS-RAS-Richtlinien unter den Eigenschaften für die jeweilige Richtlinie auf der Registerkarte **Authentifizierung** die Option **Unverschlüsselte Authentifizierung (PAP, SPAP)**.

Auswählen der RADIUS-Authentifizierungsprotokolle

Das Access Gateway unterstützt Implementierungen von RADIUS, die für die Verwendung des Password Authentication Protocol (PAP) zur Benutzerauthentifizierung konfiguriert wurden. Andere Authentifizierungsprotokolle, wie Challenge-Handshake Authentication Protocol (CHAP), werden nicht unterstützt.

Wenn Ihre Access Gateway-Bereitstellung für die Verwendung der RADIUS-Authentifizierung und Ihr RADIUS-Server für die Verwendung von PAP konfiguriert ist, können Sie eine stärkere Benutzerauthentifizierung erreichen, indem Sie dem RADIUS-Server einen starken gemeinsamen geheimen Schlüssel zuweisen. Starke gemeinsame geheime RADIUS-Schlüssel bestehen aus willkürlichen Folgen von Groß- und Kleinbuchstaben, Zahlen und Zeichen und sind mindestens 22 Zeichen lang. Verwenden Sie möglichst ein Programm, um die gemeinsamen geheimen RADIUS-Schlüssel zu generieren.

Um den Datenverkehr auf dem RADIUS-Server noch besser zu schützen, können Sie jedem Access Gateway-Gerät einen anderen gemeinsamen geheimen Schlüssel zuweisen. Wenn Sie auf dem RADIUS-Server Benutzer definieren, können Sie auch jedem Benutzer einen separaten gemeinsamen geheimen Schlüssel zuweisen. Dazu müssen Sie jeden Access Gateway-Bereich, der die RADIUS-Authentifizierung verwendet, einzeln konfigurieren. Wenn Sie die Konfigurationen mehrerer Access Gateway-Geräte in einem Cluster synchronisieren, wird allen Geräten der gleiche geheime Schlüssel zugewiesen.

Gemeinsame geheime Schlüssel werden auf dem Access Gateway konfiguriert, wenn ein RADIUS-Bereich erstellt wird.

Hinweis: Wenn Sie Access Gateway Advanced Edition verwenden, müssen Sie vor der Zuweisung von gemeinsamen geheimen RADIUS-Schlüsseln auf den Servern, auf denen die Advanced Access Control ausgeführt wird und die zum Authentifizieren der Benutzer RADIUS verwenden, ein RADIUS-Authentifizierungsprofil konfigurieren. Weitere Informationen zu Authentifizierungsprofilen finden Sie im *Administratorhandbuch für Access Gateway Advanced Edition*.

Konfigurieren der RSA SecurID-Authentifizierung

Wenn Ihre Site einen RSA ACE/Server und RSA SecurID für die Authentifizierung verwendet, können Sie das Access Gateway für die Authentifizierung des Benutzerzugriffs mit dem RSA ACE/Server konfigurieren. Das Access Gateway agiert dann als RSA-Agenthost, der sich im Namen der Benutzer authentifiziert, die sich mit Citrix Access Gateway Plug-in anmelden. Auf dem Access Gateway können mehrere RSA-Bereiche konfiguriert werden. Alle RSA-Bereiche müssen die Datei sdconf.rec verwenden und auf den gleichen RSA ACE/Server verweisen.

Das Access Gateway unterstützt RSA ACE/Server Version 5.2 und höher. Außerdem werden auch Replikationsserver unterstützt. Die Replikationsserverkonfiguration wird auf dem RSA ACE/Server vorgenommen und ist Teil der Datei sdconf.rec, die auf das Access Gateway hochgeladen wird. Wenn dies auf dem RSA ACE/Server konfiguriert ist, versucht das Access Gateway eine Verbindung zu den Replikationsservern herzustellen, falls es zu einem Ausfall oder Verlust der Netzwerkverbindung mit dem primären Server kommt.

Hinweis: Wenn Sie einen RADIUS-Server auf einem RSA-Server ausführen, konfigurieren Sie die RADIUS-Authentifizierung wie unter "Konfigurieren von RADIUS-Authentifizierung und -Autorisierung" auf Seite 90 beschrieben.

Ist ein Benutzer nicht auf dem RSA ACE/Server oder wenn die Authentifizierung auf diesem Server fehlschlägt, überprüft das Access Gateway den Benutzer anhand der lokal auf dem Access Gateway gespeicherten Benutzerinformationen, sofern auf der Registerkarte **Settings** des Bereichs die Option **Use the local user database on the Access Gateway** aktiviert ist.

Das Access Gateway unterstützt den Next-Token-Modus. Wenn ein Benutzer drei falsche Kennwörter eingibt, fordert das Citrix Access Gateway Plug-in den Benutzer auf, mit der nächsten Anmeldung so lange zu warten, bis der nächste Tokencode aktiv ist. Der RSA-Server kann so konfiguriert werden, dass das Konto eines Benutzers, der sich zu oft mit einem falschen Kennwort anmeldet, deaktiviert wird.

Für die Kontaktaufnahme mit dem RSA ACE/Server muss das Access Gateway eine Kopie der ACE-Agent-Host-Konfigurationsdatei sdconf.rec enthalten, die vom RSA ACE/Server angelegt wird. Im Folgenden wird beschrieben, wie diese Datei anzulegen und hochzuladen ist.

Hinweis: In den folgenden Schritten werden die unbedingt erforderlichen Einstellungen für das Access Gateway beschrieben. Darüber hinaus können sitespezifische Zusatzeinstellungen vorgenommen werden. Weiterführende Informationen finden Sie in der RSA ACE/Server-Produktdokumentation.

Wählen Sie beim Erstellen der Datei sdconf.rec die folgenden Einstellungen aus:

- Erstellen Sie einen Agenthost.
- Geben Sie einen beschreibenden Namen für das Access Gateway ein, das als der Agenthost fungiert, für den Sie die Konfigurationsdatei erstellen.
- Verwenden Sie als Netzwerkadresse die interne IP-Adresse des Access Gateways.
- Der Agenttyp ist "UNIX Agent".
- Stellen Sie sicher, dass bei der Erstellung des Agenthosts die Option **Node Secret Created** auf dem RSA ACE/Server deaktiviert ist. Der RSA ACE/Server sendet das Node Secret zu dem Zeitpunkt an das Access Gateway, zu dem er das erste Mal eine vom Access Gateway stammende Anforderung authentifiziert. Danach ist die Option **Node Secret Created** aktiviert. Durch Deaktivieren der Option und Generieren und Hochladen einer neuen Konfigurationsdatei können Sie den RSA ACE/Server dazu zwingen, ein neues Node Secret an das Access Gateway zu senden.
- Es gibt zwei Möglichkeiten, festzulegen, welche Benutzer sich über das Access Gateway authentifizieren können.
    - Konfigurieren Sie das Access Gateway als offenen Agenthost, der für alle lokal bekannten Benutzer offen ist.
    - Legen Sie die zu authentifizierenden Benutzer fest, indem Sie den Agenthost bearbeiten und die zu aktivierenden Benutzer auswählen.

Nachdem Sie die Einstellungen auf dem RSA-Server vorgenommen haben, erstellen Sie die Datei sdconf.rec. Die von Ihnen erstellte Datei (sdconf.rec) wird auf das Access Gateway hochgeladen.

Weitere Informationen zum Konfigurieren der Einstellungen auf dem RSA-Server finden Sie in der Dokumentation des Herstellers.

So konfigurieren Sie RSA SecurID-Authentifizierung

1. Klicken Sie auf die Registerkarte **Authentication**.
2. Geben Sie unter **Add an Authentication Realm** in das Feld **Realm name** einen Namen, der auf den RSA ACE/Server hinweist, ein.
3. Wählen Sie **One Source** und klicken Sie auf **Add**.

Hinweis: Wenn der Bereich "Default" RSA-Authentifizierung verwenden soll, entfernen Sie den Bereich "Default" wie unter "So können Sie den Bereich "Default" entfernen und neu erstellen" auf Seite 75 beschrieben.

---

4. Aktivieren Sie im Dialogfeld **Select Authentication Type** unter **Authentication type** die Option **RSA** SecurID Authentication und klicken Sie auf **OK**.

Achtung: Wenn die auf das Access Gateway hochgeladene Datei sdconf.rec ungültig ist, sendet das Access Gateway u. U. Meldungen an nicht vorhandene IP-Adressen. Netzwerküberwachungseinrichtungen könnten dies als Netzwerkspamming einstufen.

---

5. Klicken Sie zum Hochladen der soeben generierten Datei sdconf.rec auf der Registerkarte **Authentication** auf **Upload sdconf.rec File**, gehen Sie zu der Datei und klicken Sie dann auf **Öffnen**.

   Die Datei sdconf.rec wird normalerweise unter ace\data\config_files und windows\system32 gespeichert.

   - Aus der Dateistatusmeldung geht hervor, ob die Datei sdconf.rec bereits hochgeladen wurde. Wenn dies der Fall ist und Sie diese Datei ersetzen müssen, klicken Sie auf **Upload sdconf.rec File.** Gehen Sie zu der Datei und klicken Sie auf **Öffnen**, um die Datei hochzuladen.
   - Wenn Benutzer sich das erste Mal authentifizieren, schreibt der RSA ACE/Server einige Konfigurationsdateien auf das Access Gateway. Wird anschließend die IP-Adresse des Access Gateways geändert, klicken Sie auf **Remove ACE Configuration Files**, führen Sie nach entsprechender Aufforderung einen Neustart durch und laden Sie dann eine neue Datei sdconf.rec hoch. Es werden die Dateien sdconf.rec, securid und sdstatus entfernt.

6. Klicken Sie auf **Submit**.

Für die RSA SecureID-Authentifizierung können Sie die folgenden Autorisierungstypen verwenden:

- RADIUS-Autorisierung
- Lokale Autorisierung
- LDAP-Autorisierung
- Keine Autorisierung

Konfigurieren der RSA-Einstellungen für einen Cluster

Wenn Sie zwei oder mehr Geräte als Cluster konfiguriert haben, muss die Datei sdconf.rec die vollqualifizierten Domänennamen aller Geräte enthalten. Die Datei sdconf.rec wird auf einem Access Gateway installiert und dann veröffentlicht. Dadurch können alle Geräte eine Verbindung zum RSA-Server herstellen.

Sie können auch einschränken, mit welchen Geräten die Benutzer Verbindungen zum RSA-Server herstellen können. Beispiel: Ihr Cluster besteht aus drei Geräten. Wenn die vollqualifizierten Domänennamen des ersten und des zweiten Geräts in der Datei sdconf.rec enthalten sind, der des dritten Geräts aber nicht, können die Benutzer nur mit den ersten beiden Geräten Verbindungen zum RSA-Server herstellen.

Zurücksetzen des Node Secrets

Wenn Sie die Konfiguration des Access Gateways mit einer gespeicherten Konfigurationsdatei wiederhergestellt und dabei dieselbe IP-Adresse wie vorher verwendet haben, müssen Sie das Node Secret auf dem RSA ACE/Server auch zurücksetzen. Da die Konfiguration des Access Gateways wiederhergestellt wurde, gibt es auf dem kein Node Secret mehr, sodass jeder Versuch der Authentifizierung mit dem RSA ACE/Server fehlschlägt.

Nachdem Sie den gemeinsamen geheimen Schlüssel auf dem RSA ACE/Server zurückgesetzt haben, wird der RSA ACE/Server beim nächsten Authentifizierungsversuch aufgefordert, ein Node Secret an das Access Gateway zu senden.

Konfigurieren der Authentifizierung mit Secure Computing SafeWord

Die Secure Computing SafeWord-Produktlinie bietet sichere Authentifizierung mit tokenbasierten Passcodes. Nach einmaliger Verwendung wird der Passcode von SafeWord sofort ungültig gemacht und kann nicht mehr verwendet werden.

Wenn das Access Gateway das Secure Gateway während einer Secure Gateway- und Webinterface-Bereitstellung ersetzt, können Sie die Authentifizierung auf dem Access Gateway deaktivieren und dem Webinterface weiterhin erlauben, für den eingehenden HTTP-Verkehr die SafeWord-Authentifizierung bereitzustellen. Weitere Informationen über die Konfiguration des Webinterface finden Sie in der *Citrix Access Gateway Standard Edition – Integrationsdokumentation für Citrix XenApp und Citrix XenDesktop*.

Das Access Gateway unterstützt SafeWord-Authentifizierung für die folgenden Secure Computing Produkte:

- SafeWord PremierAccess
- SafeWord for Citrix
- SafeWord RemoteAccess

Es gibt mehrere Möglichkeiten, das Access Gateway für die Authentifizierung mit den SafeWord-Produkten von Secure Computing zu konfigurieren:

- Authentifizierung mit einem PremierAccess RADIUS-Server, der zusammen mit SafeWord PremierAccess installiert und für die Authentifizierung zugelassen wird.
- Authentifizierung mit einem SafeWord-IAS-Agent, der eine Komponente von SafeWord RemoteAccess, SafeWord for Citrix und SafeWord PremierAccess 4.0 ist.
- Installation des SafeWord-Webinterface-Agents, der mit dem Citrix Webinterface zusammenarbeitet. Die Authentifizierung muss nicht auf dem Access Gateway konfiguriert werden und kann vom Citrix Webinterface übernommen werden. In dieser Konfiguration werden weder der PremierAccess RADIUS-Server noch der SafeWord-IAS-Agent verwendet.

Konfigurieren der SafeWord-Einstellungen auf dem Access Gateway

Bei der Konfiguration des SafeWord-Servers benötigen Sie folgende Informationen:

- IP-Adresse des Access Gateways. Diese sollte mit der in der Clientkonfiguration des RADIUS-Servers konfigurierten Adresse übereinstimmen.
- Gemeinsamer geheimer Schlüssel. Dieser geheime Schlüssel ist auch auf der Registerkarte **Authentication** auf dem Access Gateway konfiguriert.
- IP-Adresse und Port des SafeWord-Servers.

Konfigurieren Sie einen SafeWord-Bereich zum Authentifizieren der Benutzer. Das Access Gateway agiert als SafeWord-Agent, der im Namen der Benutzer authentifiziert wird, die sich mit dem Access Gateway Plug-in angemeldet haben. Ist ein Benutzer nicht auf dem SafeWord-Server oder schlägt die Authentifizierung fehl, überprüft das Access Gateway den Benutzer anhand der lokalen Benutzerliste, sofern die Option **Use the local user database on the Access Gateway** auf der Registerkarte **Settings** aktiviert ist.

Wenn SafeWord als Bereich "Default" verwendet werden soll, entfernen Sie den aktuellen Bereich "Default" und erstellen Sie sofort einen neuen Bereich wie unter "So können Sie den Bereich "Default" entfernen und neu erstellen" auf Seite 75 beschrieben.

So konfigurieren Sie SafeWord auf dem Access Gateway

1. Klicken Sie im Administration Tool auf die Registerkarte **Authentication**.
2. Geben Sie unter **Add an Authentication Realm** in das Feld **Realm name** einen Namen ein.
3. Wählen Sie **One Source** und klicken Sie dann auf **Add**.
4. Wählen Sie unter **Authentication type** die Option **SafeWord authentication** und klicken Sie auf **OK**.

5. Geben Sie unter **Primary SafeWord Server Settings** die folgenden Daten ein:

   - Geben Sie unter **IP address** die IP-Adresse des SafeWord-Servers ein.
   - Geben Sie unter **Port** die Portnummer für den SafeWord RADIUS-Server ein. Der Standardwert ist 1812.

     Dieser Port muss mit der auf dem RADIUS-Server konfigurierten Portnummer übereinstimmen.
   - Geben Sie unter **Server secret** einen gemeinsamen geheimen RADIUS-Schlüssel ein.

     Der gemeinsame geheime Schlüssel muss mit dem auf dem RADIUS-Server konfigurierten Schlüssel übereinstimmen.

6. Wenn ein zweiter SafeWord-Server vorhanden ist, konfigurieren Sie die Einstellungen unter **Secondary SafeWord Server Settings**.

Konfigurieren der Autorisierung mit SafeWord

Wenn die Authentifizierung mit SafeWord erfolgt, können Sie die folgenden Autorisierungsverfahren verwenden:

- LDAP
- Lokale Benutzerliste
- RADIUS
- Keine Autorisierung

Informationen zum Konfigurieren der LDAP-Autorisierung finden Sie unter "Konfigurieren der LDAP-Autorisierung" auf Seite 86. Informationen zum Konfigurieren der RADIUS-Autorisierung finden Sie unter "Konfigurieren von RADIUS-Authentifizierung und -Autorisierung" auf Seite 90.

Durch entsprechende Konfiguration des SafeWord-Servers kann eingestellt werden, dass SafeWord die Gruppenmitgliedschaftsattribute zurückgibt. Weitere Informationen finden Sie in der Produktdokumentation.

Konfigurieren der Gemalto Protiva-Authentifizierung

Protiva ist eine Plattform für eine starke Authentifizierung, die entwickelt wurde, um die Stärken der Gemalto-Smartcard-Authentifizierung zu nutzen. Mit Protiva melden sich Benutzer mit einem Benutzernamen, einem Kennwort und einem zweiten Kennwort an, das nur einmal gilt und von dem Protiva-Gerät generiert wird. Ähnlich wie bei RSA SecurID wird die Authentifizierungsanfrage an den Protiva-Authentifizierungsserver gesendet und das Kennwort wird entweder bestätigt oder verworfen.

Konfigurieren der Gemalto Protiva-Einstellungen

Verwenden Sie beim Konfigurieren von Gemalto Protiva für Access Gateway die folgende Richtschnur:

- Installieren Sie den Protiva-Server.
- Installieren Sie das Protiva Internet Authentication Server (IAS) Agent Plug-in auf einem Microsoft IAS RADIUS-Server. Notieren Sie sich die IP-Adresse und die Portnummer des IAS-Servers.
- Konfigurieren Sie einen Bereich (realm) auf dem Access Gateway für die RADIUS-Authentifizierung und geben Sie die Einstellungen des Protiva-Servers an.

So konfigurieren Sie einen Gemalto Protiva-Bereich

1. Klicken Sie im Administration Tool auf die Registerkarte **Authentication**.
2. Geben Sie unter **Add an Authentication Realm** in das Feld **Realm name** einen Namen ein.
3. Wählen Sie **One Source** und klicken Sie dann auf **Add**.

Hinweis: Wenn Sie Zweimethodenauthentifizierung konfigurieren, wählen Sie **Two Source** aus und klicken Sie auf **Add**. Weitere Informationen zum Konfigurieren der Zweimethodenauthentifizierung finden Sie unter "Konfigurieren von Zweimethodenauthentifizierung" auf Seite 108.

---

4. Wählen Sie unter **Select Authentication Type** neben **Authentication type** die Option **Gemalto authentication** aus und klicken Sie auf **OK**.
5. Geben Sie unter **IP Address** die IP-Adresse des RADIUS IAS-Servers ein.
6. Geben Sie im Feld **Port** die Portnummer ein.
7. Geben Sie in das Feld **Server secret** das Node Secret des RADIUS IAS-Servers ein und klicken Sie auf **Submit**.

Konfigurieren von NTLM-Authentifizierung und -Autorisierung

Das Access Gateway kann so konfiguriert werden, dass Benutzer mit NTLM-Authentifizierung (Windows NT LAN Manager) anhand der Benutzerdatenbank auf einem Windows NT 4.0-Domänencontroller authentifiziert werden.

Ist ein Benutzer nicht in der Benutzerdatenbank auf den Windows NT 4.0-Domänencontrollern oder schlägt die Authentifizierung fehl, kann das Access Gateway den Benutzernamen anhand der lokalen Benutzerliste auf dem Access Gateway überprüfen und den Benutzer anhand der lokalen Liste authentifizieren, sofern das Kontrollkästchen **Use the local user database on the Access Gateway** auf der Registerkarte **Settings** aktiviert ist.

Ein Windows NT 4.0-Domänencontroller unterhält Domänenbenutzerkonten in einer Datenbank auf dem Windows NT 4.0-Server. Ein Domänenbenutzerkonto umfasst einen Benutzernamen und ein Kennwort sowie weitere Informationen über den Benutzer.

Zum Konfigurieren der NTLM-Authentifizierung erstellen Sie einen NTLM-Authentifizierungsbereich, in dem die Adresse und der Port hinterlegt sind, den das Access Gateway zum Herstellen einer Verbindung zum Windows NT 4.0-Domänencontroller verwendet. Außerdem geben Sie einen Timeoutwert an, mit dem festgelegt wird, in welcher Zeit eine Authentifizierung beim Server abgeschlossen sein muss.

Wenn sich Benutzer am Access Gateway anmelden, geben sie die Anmeldeinformationen (Benutzername und Kennwort) ein, die im Domänenbenutzerkonto auf dem Windows NT 4.0-Server hinterlegt sind. Das Access Gateway stellt eine Verbindung zum Windows NT 4.0-Server her und übergibt diese Anmeldeinformationen an den Server. Der Server authentifiziert den Benutzer.

So konfigurieren Sie NTLM-Authentifizierung

1. Klicken Sie auf die Registerkarte **Authentication**.
2. Geben Sie unter **Add an Authentication Realm** in das Feld **Realm name** einen Namen für den Authentifizierungsbereich ein.

   Wenn Ihre Site mehrere Authentifizierungsbereiche besitzt, sollten Sie einen Namen verwenden, aus dem deutlich der NTLM-Bereich hervorgeht, für den Sie die Einstellungen festlegen. Bei Bereichsnamen ist auf die Groß- und Kleinschreibung zu achten. Darüber hinaus können sie Leerzeichen enthalten.

   Hinweis: Wenn der Bereich "Default" NTLM-Authentifizierung verwenden soll, entfernen Sie den Bereich "Default" wie unter "So können Sie den Bereich "Default" entfernen und neu erstellen" auf Seite 75 beschrieben.

   ---

3. Wählen Sie **One Source** und klicken Sie auf **Add**.
4. Wählen Sie im Dialogfeld **Select Authentication Type** unter **Authentication type** die Option **NTLM authentication** und klicken Sie auf **OK**.
5. Geben Sie im Dialogfeld für den Bereich (realm) unter **IP address or FQDN** die IP-Adresse des Windows NT 4.0-Domänencontrollers ein.
6. Geben Sie im Feld **Port** die Nummer des Ports ein, den der Windows NT 4.0-Domänencontroller nach NTLM-Authentifizierungsverbindungen abhört.

   Der Standardport für NTLM-Authentifizierungsverbindungen ist 139.

   Hinweis: Wenn als Port 0 (Null) eingegeben wird, versucht das Access Gateway, automatisch eine Portnummer für die Verbindung zu ermitteln.

   ---

7. Geben Sie im Feld **Time-out (in seconds)** die Zeitspanne in Sekunden ein, innerhalb derer die Authentifizierung abgeschlossen sein muss. Wird die Authentifizierung nicht innerhalb dieses Zeitraums abgeschlossen, schlägt sie fehl. Klicken Sie auf **Submit**.

Konfigurieren der NTLM-Autorisierung

Ein Windows NT 4.0-Domänencontroller unterhält Gruppenkonten. Ein Gruppenkonto besteht aus mehreren Domänenkonten einzelner Benutzer (und anderen Konten).

Zum Konfigurieren der NTLM-Autorisierung klicken Sie im Authentifizierungsbereich auf die Registerkarte **Authorization** und geben die Adresse und den Port ein, den das Access Gateway zum Herstellen einer Verbindung zum Windows NT 4.0-Domänencontroller verwendet. Außerdem geben Sie einen Timeoutwert an, der festlegt, in welcher Zeit eine Autorisierung am Windows NT-Server abgeschlossen sein muss.

Wenn ein Benutzer erfolgreich authentifiziert wurde, gibt der Domänencontroller eine Liste aller globalen Gruppen, denen der authentifizierte Benutzer angehört, an das Access Gateway zurück.

Das Access Gateway prüft dann, ob auf dem Access Gateway ein Benutzergruppenname existiert, der mit einer globalen Windows NT 4.0-Gruppe übereinstimmt, der der Benutzer angehört. Wenn das Access Gateway eine Übereinstimmung findet, erhält der Benutzer die Zugangsrechte zu den internen Netzwerken, die der Benutzergruppe auf dem Access Gateway zugeordnet sind.

So konfigurieren Sie NTLM-Autorisierung

1. Klicken Sie auf die Registerkarte **Authentication** und öffnen Sie den Bereich, für den Sie NTLM-Autorisierung aktivieren möchten.
2. Klicken Sie auf die Registerkarte **Authorization**.
3. Wählen Sie unter **Authorization type** die Option **NTLM authorization**.
4. Geben Sie im Feld **Server IP Address or FQDN** den vollqualifizierten Domänennamen oder die IP-Adresse des Windows NT 4.0-Domänencontrollers ein, der die NTLM-Autorisierung durchführen wird.
5. Geben Sie im Feld **Server Port** die Portnummer ein.

   Der Standardport für NTLM-Authentifizierungsverbindungen ist 139.

   Hinweis: Wenn als Port 0 (Null) eingegeben wird, versucht das Access Gateway, automatisch eine Portnummer für die Verbindung zu ermitteln.

   ---

6. Geben Sie im Feld **Time-out (in seconds)** die Zeitspanne in Sekunden ein, innerhalb derer die Autorisierung abgeschlossen sein muss, bevor der Authentifizierungsversuch abgebrochen wird.
7. Klicken Sie auf **Submit**.

Konfigurieren von erweiterten Optionen für die Authentifizierung

Für die RADIUS-, SafeWord- oder Gemalto Protiva-Authentifizierung können Sie erweiterte Authentifizierungsoption konfigurieren. Zu den erweiterten Optionen gehören:

- Konfigurieren des Benutzernamenpräfixes
- Konfigurieren von Einmal-Kennwörtern
- Verbergen der Aufforderung für die Antwortüberprüfung

Diese Optionen werden im Authentifizierungsbereich für jeden Authentifizierungstyp konfiguriert.

Konfigurieren des Benutzernamenpräfixes

Sie können die Authentifizierungsrichtlinie so konfigurieren, dass Benutzer sich mit dem UPN (user principle name) anmelden, der das Format *benutzername@domäne.com* hat.

Wenn Sie den UPN für die LDAP-Authentifizierung konfigurieren, geben Sie für den LDAP-Authentifizierungsbereich unter **Administrator bind DN** *RADIUSkonto@domänenname.com* ein, wobei domänenname.com der Name Ihrer Domäne ist. Geben Sie in das Feld **Server logon name attribute** den *UPN* ein.

Wenn Sie RADIUS, SafeWord oder Gemalto Protiva verwenden, geben Sie im Authentifizierungsbereich unter **Advanced Options** *benutzername@domäne.com*.

Konfigurieren der Authentifizierung für die Verwendung von Einmal-Kennwörtern

Wenn die Authentifizierung auf dem Access Gateway so konfiguriert ist, dass Einmal-Kennwörter (beispielsweise von einem RSA SecurID-Token) mit RADIUS verwendet werden, versucht das Access Gateway, Benutzer mit dem gecachten Kennwort neu zu authentifizieren. Dies passiert, wenn mit dem Administration Tool Änderungen am Access Gateway gemacht wurden oder wenn die Verbindung zwischen dem Access Gateway Plug-in und dem Access Gateway unterbrochen und wiederhergestellt wurde.

Es kann auch vorkommen, wenn Benutzerverbindungen für die Verwendung von Citrix XenApp Plug-ins konfiguriert sind und die Verbindung zum Webinterface mit RADIUS oder LDAP hergestellt wird. Wenn Benutzer eine Anwendung starten und verwenden, dann zum Webinterface zurückkehren, um eine andere Anwendung zu starten, verwendet das Access Gateway gecachte Informationen, um die Benutzer zu authentifizieren.

Sie können verhindern, dass Einmal-Kennwörter im Cache gespeichert werden, Benutzer müssen dann ihre Anmeldeinformationen noch einmal eingeben.

Wenn Sie RSA SecurID, Gemalto Protiva oder SafeWord als Authentifizierungstyp verwenden ist diese Einstellung standardmäßig aktiviert und kann nicht geändert werden. Wenn Sie RADIUS verwenden, ist diese Einstellung standardmäßig deaktiviert, Sie können sie aber aktivieren.

So verhindern Sie das Cachen von Einmal-Kennwörtern

1. Klicken Sie im Administration Tool auf die Registerkarte **Authentication**.
2. Öffnen Sie den Authentifizierungsbereich, der das Einmal-Kennwort verwendet.
3. Wählen Sie **Use the password one time** und klicken Sie auf **Submit**.

Verbergen der Aufforderung für die Antwortüberprüfung

Wenn Sie die RADIUS-Authentifizierung verwenden und in Ihrer Bereitstellung Challenge/Response eingesetzt wird, erhalten Benutzer zwei Überprüfungsaufforderungen für die Antwort. Sie verhindern mit dieser Einstellung, dass die zweite Aufforderung angezeigt wird. Dies gilt für RADIUS-Bereitstellungen mit SafeWord und Gemalto Protiva.

So verbergen Sie die Antwortsaufforderung

Wählen Sie im RADIUS-, SafeWord- oder Gemalto Protiva-Authentifizierungsbereich unter **Advanced Options** die Option **Hide the Verify Response prompt** und klicken Sie auf **Submit**.

Konfigurieren von Zweimethodenauthentifizierung

Das Access Gateway unterstützt Zweimethodenauthentifizierung, bei der sich Benutzer mit zwei Authentifizierungstypen anmelden müssen. Sie haben auf der Registerkarte **Authentication** die Möglichkeit, für einen Bereich zwei Authentifizierungsmethoden zu konfigurieren, z. B. LDAP und SafeWord.

Der Bereich "Default" kann für die Zweimethodenauthentifizierung konfiguriert werden. Es können Bereiche mit einer Authentifizierungsmethode und Bereiche mit Zweimethodenauthentifizierung nebeneinander bestehen. So können Sie z. B. einen oder mehrere Bereich(e) für ein einzelnes Authentifizierungsverfahren und zusätzlich einen oder mehrere Bereich(e) einrichten, die für Zweimethodenauthentifizierung konfiguriert sind. In einer gemischten Authentifizierungsumgebung sehen Benutzer bei der Anmeldung zwei Kennwortfelder. Wenn sich Benutzer mit nur einem Authentifizierungstyp anmelden, bleibt das zweite Kennwortfeld leer.

So erstellen und konfigurieren Sie einen Bereich mit Zweimethodenauthentifizierung

1. Klicken Sie auf die Registerkarte **Authentication**.
2. Geben Sie unter **Add an Authentication Realm** in das Feld **Realm name** einen Namen ein.
3. Wählen Sie **Two Source** und klicken Sie dann auf **Add**.
4. Legen Sie im Dialogfeld **Select Authentication Type** unter **Primary authentication type** und **Secondary authentication type** das jeweilige Authentifizierungsverfahren fest. Klicken Sie auf **OK**.
5. Konfigurieren Sie auf der Registerkarte **Primary Authentication** die Einstellungen für den ersten Authentifizierungstyp und klicken Sie auf **Submit**.
6. Konfigurieren Sie auf der Registerkarte **Secondary Authentication** die Einstellungen für den zweiten Authentifizierungstyp und klicken Sie auf **Submit**.
7. Wählen Sie auf der Registerkarte **Authorization** unter **Authorization type** den gewünschten Autorisierungstyp aus, konfigurieren Sie die Einstellungen und klicken Sie auf **Submit**.

Bei der Zweimethodenauthentifizierung wird die primäre Authentifizierung zuerst überprüft. Ist diese erfolgreich, wird die sekundäre Authentifizierung geprüft. Wenn Sie z. B. auf der Registerkarte **Secondary Authentication** RSA SecurID und auf der Registerkarte **Primary Authentication** LDAP konfiguriert haben, müssen die Benutzer beim Anmelden in das erste Kennwortfeld ihr LDAP-Kennwort und in das zweite Kennwortfeld die RSA SecurID-PIN und den Passcode eingeben. Wenn Benutzer auf **Connect** klicken, nimmt das Access Gateway die Authentifizierung zuerst anhand des LDAP-Kennworts und dann anhand von RSA SecurID-PIN und des Passcode vor.

Ändern der Beschriftung von Kennwortfeldern

Die Beschriftung der Kennwortfelder kann an den Authentifizierungstyp angepasst werden, mit dem sich Benutzer anmelden, damit sie genau wissen, welches Kennwort sie eingeben müssen. Dies ist besonders dann nötig, wenn das Access Gateway für die Unterstützung von Authentifizierungstypen von Drittanbietern konfiguriert ist. Wenn Benutzer sich z. B. mit LDAP und dem starken Authentifizierungssystem Gemalto Protiva (RADIUS) authentifizieren müssen, können Sie die Kennwortfelder mit diesen Typen beschriften, damit die Benutzer wissen, was sie eingeben müssen. Statt mit **Kennwort** und **Sekundäres Kennwort** könnten die Felder z. B. mit **Windows-Domänenkennwort** und **Gemalto Protiva-Passcode** beschriftet werden. Die Beschriftungen können je nach Verwendung einzelner Authentifizierungsmethoden oder Zweimethodenauthentifizierung geändert werden.

So ändern Sie die Beschriftungen der Kennwortfelder

1. Klicken Sie auf die Registerkarte **Authentication** und unter **Add an Authentication Realm** auf **Advanced**.
2. Geben Sie in den Feldern **Password label** und **Secondary password label** die Beschriftungen für die Felder ein.
3. Klicken Sie auf **OK**.

Wenn sich Benutzer anschließend anmelden, sehen sie die neuen Feldbeschriftungen.

Konfigurieren von Netzwerkzugriff und Gruppenressourcen

Benutzer greifen über das Netzwerk auf interne Ressourcen zu. Sie können Zugriff auf beliebige Subnetze Ihres Netzwerks gewähren oder verweigern. Beispiel: Sie können einem Benutzer Zugriff auf eine Dateifreigabe auf Ihrem Netzwerk gewähren oder dem Benutzer vollen Zugriff auf alle Ressourcen im Netzwerk geben. Wenn Sie Netzwerkzugriff und Gruppenressourcen konfigurieren, erstellen Sie Zugriffssteuerungslisten. Basierend auf diesen Listen können Sie steuern, auf welche Ressourcen Benutzer zugreifen können, wenn sie eine Verbindung zum gesicherten Netzwerk herstellen.

Dieses Kapitel enthält:

- "Konfigurieren des Netzwerkrouting"
- "Bereitstellen von Netzwerkzugriff für Benutzer"
- "Konfigurieren von Benutzergruppen"
- "Konfigurieren von Ressourcen für eine Benutzergruppe"
- "Konfigurieren von Netzwerkressourcen"
- "Festlegen von Anwendungsrichtlinien"
- "Konfigurieren von Endpunktrichtlinien und -ressourcen"
- "Festlegen der Priorität von Gruppen"
- "Konfigurieren des Access Gateways für Citrix Branch Repeater"

Konfigurieren des Netzwerkrouting

Um Zugriff auf interne Netzwerkressourcen zu gewähren, muss das Access Gateway in der Lage sein, Daten an interne Netzwerke weiterzuleiten.

Die Netzwerke, an die das Access Gateway Daten weiterleiten kann, werden durch die Konfiguration der Access Gateway-Routingtabelle und das für das Access Gateway festgelegte Standardgateway bestimmt.

Wenn das Access Gateway ein Paket erhält, überprüft es die Routingtabelle. Wenn die Zieladresse des Pakets in einem Netzwerk ist, für das eine Route in der Routingtabelle vorhanden ist, wird das Paket an dieses Netzwerk weitergeleitet.

Wenn das Access Gateway ein Paket erhält und die Routingtabelle keine Route für die Zieladresse des Pakets enthält, sendet das Access Gateway das Paket von authentifizierten Benutzern an das Standardgateway. Die Routingfunktionen des Standardgateways bestimmen dann, wie das Paket weitergeleitet wird.

Die Routingtabelle des Access Gateways muss alle Routen enthalten, die zum Weiterleiten von Daten an interne Netzwerkressourcen erforderlich sind, auf die Benutzer eventuell Zugriff benötigen.

Sie legen fest, wie die Access Gateway-Routingtabelle konfiguriert werden. Sie können eine Routing Information Protocol (RIP)-Option auswählen, sodass Routen von einem RIP-Server automatisch konfiguriert werden, oder Sie können eine statische Routingoption auswählen und die Routen manuell konfigurieren. Weitere Informationen hierzu finden Sie unter "Konfigurieren von dynamischen und statischen Routen" auf Seite 60.

Bereitstellen von Netzwerkzugriff für Benutzer

Die Netzwerkressourcen, zu denen Sie Benutzern Zugriff gewähren, müssen in einem Netzwerk sein, an das das Access Gateway Daten weiterleiten kann. Sie können das Access Gateway so konfigurieren, dass entweder dynamische oder statische Routen zum Weiterleiten von Daten an interne Netzwerkressourcen verwendet werden.

Sie können mit dem Access Gateway ganz gezielt festlegen, wie Sie Benutzern Zugriff auf Netzwerkressourcen gewähren. Der Benutzerzugriff auf Netzwerkressourcen lässt sich folgendermaßen steuern:

- Sie erstellen Netzwerkressourcengruppen.

  Eine Netzwerkressourcengruppe enthält einen oder mehrere Netzwerkstandort(e). Im Allgemeinen ist eine Netzwerkressourcengruppe eine Teilgruppe aller Netzwerkressourcen, an die das Access Gateway Daten weiterleiten kann.

So kann eine Ressourcengruppe z. B. den Zugriff auf eine einzelne Anwendung, eine Gruppe von Anwendungen, einen Bereich von IP-Adressen oder das gesamte Intranet ermöglichen. Welche Elemente Sie in eine Netzwerkressourcengruppe aufnehmen, hängt in hohem Maße von den verschiedenen Zugriffsanforderungen Ihrer Benutzer ab. So kann es sein, dass Sie einigen Benutzergruppen Zugriff auf viele Ressourcen gewähren möchten, während andere Benutzergruppen lediglich auf einen kleinen Teilsatz der Ressourcen zugreifen sollen. Durch Erlauben und Verweigern des Benutzergruppenzugriffs auf Netzwerkressourcengruppen erstellen Sie eine Zugriffssteuerungsliste (Access Control List, ACL) für die betreffende Benutzergruppe.

- Sie bestimmen, ob eine Benutzergruppe ohne eine ACL vollen Zugriff auf Ressourcen in einem Netzwerk hat, an das das Access Gateway Daten weiterleiten kann.

  Standardmäßig haben Benutzergruppen ohne ACL Zugriff auf alle Ressourcen in allen Netzwerken, an die das Access Gateway Daten weiterleiten kann. Dieses Standardverhalten empfiehlt sich, wenn die meisten Ihrer Benutzergruppen vollen Netzwerkzugriff haben sollen. Bei Beibehaltung dieses Standardverhaltens müssen Sie eine Zugriffssteuerungsliste nur für die Benutzergruppen konfigurieren, die keinen vollen Netzwerkzugriff haben sollen. Das Standardverhalten kann auch für einen ersten Test der Bereitstellung nützlich sein.

  Sie können das Standardverhalten ändern, sodass Benutzergruppen der Netzwerkzugriff so lange verweigert wird, bis sie ausdrücklich berechtigt sind, auf eine oder mehrere Netzwerkressourcengruppen zuzugreifen.

- Sie konfigurieren Zugriffssteuerungslisten für Benutzergruppen, indem Sie festlegen, welche Netzwerkressourcen für die einzelnen Benutzergruppen zugänglich oder nicht zugänglich sein sollen.

  Standardmäßig ist der Zugriff auf alle Netzwerkressourcengruppen erlaubt und der Netzwerkzugriff wird durch die Option **Deny Access without access control list (ACL)** auf der Registerkarte **Global Cluster Policies** gesteuert. Wenn Sie den Zugriff auf eine Ressourcengruppe erlauben oder verweigern, wird automatisch auch der Zugriff auf alle anderen Ressourcengruppen verweigert und der Netzwerkzugriff für die Benutzergruppe wird ausschließlich über deren Zugriffssteuerungsliste gesteuert.

  Wenn eine Ressourcengruppe eine Ressource enthält, auf die eine Benutzergruppe keinen Zugriff haben soll, können Sie eine separate Ressourcengruppe nur für diese Ressource erstellen und der Benutzergruppe den Zugriff auf diese spezifische Ressource verweigern.

Die folgende Tabelle enthält eine Zusammenfassung der soeben beschriebenen Optionen.

ACL für Benutzergruppe eingerichtet	Zugriff ohne ACL verweigern	Für die Benutzergruppe zugängliche Ressourcen
Nein	Nein	Beliebiges Netzwerk, auf das das Access Gateway zugreifen kann
Ja	Nein	Erlaubte Ressourcengruppen
Nein	Ja	Kein Zugriff auf das Netzwerk
Ja	Ja	Erlaubte Ressourcengruppen

Bei der Konfiguration des Netzwerkzugriffs muss die strengste Richtlinie als erste und die schwächste Richtlinie als letzte konfiguriert werden. Beispiel: Sie möchten Zugriff auf alle Ressourcen im Netzwerk 10.0.x.x gewähren, aber Zugriff auf Netzwerk 10.0.20.x verweigern. Konfigurieren Sie als erstes Zugriff auf das Netzwerk 10.0.20.x und dann auf das Netzwerk 10.0.x.x.

Aktivieren von Split-Tunneling und zugänglichen Netzwerken

Auf der Registerkarte *Global Cluster Policies* können Sie **Split-Tunneling** aktivieren, um zu verhindern, dass das Access Gateway Plug-in unnötige Netzwerkdaten an das Access Gateway sendet.

Wenn Split-Tunneling nicht aktiviert ist, empfängt das Access Gateway Plug-in den gesamten vom Clientgerät ausgehenden Datenverkehr und leitet ihn durch den VPN-Tunnel an das Access Gateway weiter.

Wenn Sie Split-Tunneling aktivieren, sendet das Access Gateway Plug-in nur solche Daten durch den VPN-Tunnel, die für durch das Access Gateway gesicherte Netzwerke bestimmt sind. Das Access Gateway Plug-in sendet keine Daten, die für ungesicherte Netzwerke bestimmt sind, an das Access Gateway.

Wenn Sie Split-Tunneling aktivieren, müssen Sie eine Liste zugänglicher Netzwerke auf der Registerkarte **Global Cluster Policies** angeben. Die Liste der zugänglichen Netzwerke muss alle internen Netzwerke und Subnetzwerke enthalten, auf die Benutzer eventuell mit dem Access Gateway Plug-in zugreifen müssen.

Das Access Gateway Plug-in verwendet die Liste der zugänglichen Netzwerke als Filter, um zu bestimmen, ob vom Clientgerät gesendete Pakete an das Access Gateway gesendet werden sollen.

Beim Start des Access Gateway Plug-ins erhält er die Liste zugänglicher Netzwerke vom Access Gateway. Das Access Gateway Plug-in überprüft alle vom Clientgerät übertragenen Pakete und vergleicht die Adressen in den Paketen mit der Liste der zugänglichen Netzwerke. Ist die Zieladresse im Paket in einem der zugänglichen Netzwerke, sendet das Access Gateway Plug-in das Paket durch den VPN-Tunnel an das Access Gateway. Ist die Zieladresse nicht in einem zugänglichen Netzwerk, wird das Paket nicht verschlüsselt und das Plug-in leitet das Paket dementsprechend weiter.

Hinweis: Wenn Benutzer mit Citrix XenApp Plug-ins eine Verbindung zu in der Serverfarm veröffentlichten Anwendungen herstellen, muss Split-Tunneling nicht aktiviert werden.

So aktivieren Sie Split-Tunneling und zugängliche Netzwerke

1. Klicken Sie auf die Registerkarte **Global Cluster Policies**.
2. Aktivieren Sie im Bereich **Access options** die Option **Enable split tunneling**.
3. Geben Sie im Feld **Accessible networks** die Liste der Netzwerke ein, die Netzwerkressourcen enthalten, auf die Benutzer mit dem Access Gateway Plug-in zugreifen müssen. Trennen Sie dabei die einzelnen Netzwerkeinträge durch ein Leerzeichen oder einen Zeilenumbruch voneinander.
4. Klicken Sie auf **Submit**.

Konfigurieren von Benutzergruppen

Benutzergruppen definieren die Ressourcen, auf die der Benutzer zugreifen darf, wenn er über das Access Gateway eine Verbindung zum gesicherten Netzwerk herstellt. Gruppen sind mit der Liste der lokalen Benutzer verknüpft. Nach dem Hinzufügen lokaler Benutzer zu einer Gruppe können Sie auf der Registerkarte **Access Policy Manager** die Ressourcen definieren, auf die diese Benutzer Zugriff haben sollen. Weitere Informationen zum Konfigurieren von lokalen Benutzern finden Sie unter "Konfigurieren lokaler Benutzer" auf Seite 79.

Wenn Sie die Autorisierung auf dem Access Gateway aktivieren, werden die Benutzergruppeninformationen nach dem Authentifizieren des Benutzers vom Authentifizierungsserver abgerufen. Wenn der vom Authentifizierungsserver abgerufene Gruppenname mit einem lokal auf dem Access Gateway erstellten Gruppennamen übereinstimmt, werden die Eigenschaften der lokalen Gruppe für die vom Authentifizierungsserver abgerufene Gruppe verwendet.

Wichtig: Die Gruppennamen auf den Authentifizierungsservern und auf dem Access Gateway müssen identisch sein (auch hinsichtlich der Groß- und Kleinschreibung).

Konfigurieren von Zugriffssteuerungslisten

Jeder Benutzer sollte mindestens einer Gruppe angehören, die lokal auf dem Access Gateway definiert ist. Wenn Benutzer keiner Gruppe angehören, wird anhand von Zugriffssteuerungslisten bestimmt, auf welche Ressourcen der Benutzer Zugriff hat. Diese Zugriffssteuerungslisten können mit der Option **Deny access without access control list (ACL)** folgendermaßen angepasst werden:

- Wenn die Option "Deny Access" aktiviert ist, können Benutzer keine Verbindung herstellen.
- Wenn die Option "Deny Access" deaktiviert ist, haben Benutzer vollen Zugriff auf das Netzwerk.

So verweigern Sie Benutzergruppen ohne Zugriffssteuerungsliste den Zugriff

1. Klicken Sie auf die Registerkarte **Global Cluster Policies**.
2. Klicken Sie im Bereich **Access Options** auf **Deny access without access control list (ACL)** und klicken Sie auf **Submit**.

Erstellen lokaler Benutzergruppen

Sie können auch lokale Gruppen hinzufügen, die in keiner Beziehung zu Gruppen auf den Authentifizierungsservern stehen. So können Sie z. B. eine lokale Gruppe erstellen, um einen Vertragspartner oder Besucher einzurichten, der vorübergehend Zugriff haben soll. Es muss dafür auf dem Authentifizierungsserver kein Eintrag erstellen werden. Informationen zum Erstellen eines lokalen Benutzers finden Sie unter "Konfigurieren lokaler Benutzer" auf Seite 79.

Hinweis: Wenn Sie eine Benutzergruppe mit mehr als 127 Zeichen erstellen und diese Gruppe anschließend löschen, wird sie dennoch weiterhin auf der Registerkarte **Group Priority** angezeigt. Sie können dieses Problem umgehen, indem Sie Benutzergruppennamen mit weniger als 127 Zeichen verwenden. Alle Zeichen, die diese Grenze überschreiten, werden abgeschnitten.

Konfigurieren von Ressourcengruppen

Eine Reihe von Aspekten des Access Gateway-Betriebs wird auf Gruppenebene konfiguriert. Dabei wird zwischen Gruppeneigenschaften und Gruppenressourcen unterschieden.

Zu den Gruppeneigenschaften gehören Folgende:

- Gruppen, die die Eigenschaften der Standardgruppe übernehmen.
- Neuanmeldung durch die Benutzer, wenn es zu einer Netzwerkunterbrechung gekommen ist oder wenn der Computer im Standby-Modus oder Ruhezustand war.
- Aktivieren der Single Sign-On-Funktionalität unter Windows.
- Aktivieren von Single Sign-On für das Webinterface.
- Ausführen von Anmeldeskripten, wenn Benutzer sich mit Domänenanmeldeinformationen anmelden.
- Verweigern des Zugriffs auf Anwendungen im Netzwerk ohne definierte Anwendungsrichtlinie.
- Zugriffskonfiguration zum Festlegen der Zeitdauer für eine Sitzung. Es gibt drei Arten von Sitzungstimeouts:
    - Benutzersitzungstimeout: Hiermit wird festgelegt, wie lange Benutzer angemeldet bleiben können, unabhängig davon ob Aktivität stattfindet. Die angegebene Zeit ist absolut. Wenn für Benutzer ein Timeout von 60 Minuten festgelegt ist, endet die Sitzung nach 60 Minuten. 1 Minute vorher werden die Benutzer in einer Warnmeldung auf das nahende Sitzungsende hingewiesen.
    - Netzwerkaktivitätstimeout: Hierbei werden Benutzer nach einer bestimmten Zeitspanne abgemeldet, wenn keine Netzwerkaktivität vom Clientgerät durch den VPN-Tunnel festgestellt wurde. Netzwerkaktivität vom LAN wird nicht berücksichtigt.
    - Timeout bei inaktiver Sitzung: Hierbei wird Netzwerkaktivität festgestellt, aber keine Benutzeraktivität. Benutzeraktivitäten sind Tastatureingaben oder Mausbewegungen.

- Aktivieren von Split DNS: Hierbei sendet das Clientgerät Namensauflösungsanfragen and den Access Gateway-DNS-Server und den lokalen DNS-Server des Clients.
- IP-Pooling, wenn jedem Client eine eindeutige IP-Adresse zugewiesen ist.
- Anmelde- und Portalseitenverwendung, womit definiert wird, welche Seite Benutzern bei der Anmeldung angezeigt wird. Die Anmeldeseite kann entweder eine von Citrix bereitgestellte Seite oder eine auf das einzelne Unternehmen zugeschnittene Seite sein. Wenn Ihr Unternehmen Citrix XenApp oder Citrix XenDesktop verwendet, kann die Anmeldeseite das Webinterface sein. Wenn Sie Benutzern mehrere Optionen zur Anmeldung geben möchten, verwenden Sie die Clientoptionenseite. Weitere Informationen hierzu finden Sie unter "Konfigurieren einer Portalseite mit mehreren Anmeldeoptionen" auf Seite 178.

Zu den Gruppenressourcen gehören:

- Netzwerkressourcen, die die Netzwerke definieren, zu denen die Benutzer eine Verbindung herstellen können.
- Anwendungsrichtlinien, die die Anwendungen definieren, die die Benutzer bei der Verbindungsherstellung verwenden können. Neben dem Auswählen der Anwendung können Sie auch definieren, auf welche Netzwerke die Anwendung zugreifen kann und ob beim Herstellen einer Verbindung Endpunktrichtlinien erfüllt werden müssen.
- Endpunktressourcen und -richtlinien, die die erforderlichen und die optionalen Parameter definieren, die auf den Benutzercomputern beim Anmelden vorhanden sein müssen.

Wenn Benutzer zu mehreren Gruppen gehören, werden die Gruppenrichtlinien, nach den auf der Registerkarte **Group Priority** festgelegten Gruppenpriorität angewendet. Informationen zum Festlegen der Gruppenprioritäten finden Sie unter "Festlegen der Priorität von Gruppen" auf Seite 134.

Erstellen von Benutzergruppen

Benutzergruppen werden auf der Registerkarte **Access Policy Manager** erstellt. Es ist möglich, mehrere Benutzergruppen zu erstellen und zu konfigurieren. Beim Erstellen einer neuen Gruppe wird die Eigenschaftenseite angezeigt, auf der Sie die Einstellungen für die Gruppe konfigurieren können. Wenn alle Einstellungen festgelegt sind, können der Gruppe Ressourcen hinzugefügt werden.

So erstellen Sie eine lokale Benutzergruppe auf dem Access Gateway

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Klicken Sie mit der rechten Maustaste im linken Bereich auf **User Groups** und klicken Sie dann auf **New Group**.

   Geben Sie unter **Group Name** einen aussagekräftigen Namen für die Gruppe ein (z. B. "Temp. Mitarbeiter" oder "Buchhaltung") und klicken Sie dann auf **OK**.

   Wichtig: Wenn die Eigenschaften der Gruppe für die Authentifizierung bei Authentifizierungsservern verwendet werden sollen, muss der Gruppenname mit dem Gruppennamen auf dem Authentifizierungsserver identisch sein (auch hinsichtlich der Groß- und Kleinschreibung und der verwendeten Leerzeichen).

   Ein Dialogfeld für die hinzugefügte Gruppe wird geöffnet.
3. Informationen zum Konfigurieren der Gruppe finden Sie unter "Konfigurieren von Ressourcen für eine Benutzergruppe" auf Seite 120.

So entfernen Sie eine Benutzergruppe

Klicken Sie mit der rechten Maustaste im linken Bereich der Registerkarte **Access Policy Manager** auf eine Gruppe und klicken Sie dann auf **Delete**.

Eigenschaften der Standardgruppe ("Default")

Wenn die einzige auf dem Access Gateway konfigurierte Gruppe die Standardbenutzergruppe ist, erhalten alle lokalen Benutzer die für diese Gruppe konfigurierten Einstellungen. Sie können den Zugriff einschränken, indem Sie zusätzliche Gruppen auf dem Access Gateway konfigurieren und dann entscheiden, ob sie denselben Zugriff wie die Standardbenutzergruppe erhalten sollen.

Beispiel: Zwei Benutzer gehören einer Gruppe temporärer Mitarbeiter an. Sie dürfen Verbindungen zu bestimmten internen Ressourcen, z. B. einem Exchange-Server und einem Dateiserver, herstellen. Wenn sie die Einstellungen der Standardgruppe erben, erhalten sie dadurch unter Umständen Zugriff auf Ressourcen, die nur für festangestellte Mitarbeiter bestimmt sind.

In den Benutzergruppeneigenschaften können Sie festlegen, ob Benutzer die Einstellungen der Standardgruppe erben sollen. Für die Standardgruppe ist diese Option nicht verfügbar.

So aktivieren oder deaktivieren Sie die Eigenschaften der Gruppe "Default"

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Klicken Sie mit der rechten Maustaste im linken Bereich auf die Benutzergruppe und klicken Sie dann auf **Properties**.
3. Auf der Registerkarte **General** wählen Sie eine dieser Optionen:
   - Wenn die Benutzer die Einstellungen der Standardgruppe nicht erben sollen, deaktivieren Sie die Option **Inherit properties from the Default group**.
   - Wenn die Benutzer die Einstellungen der Standardgruppe erben sollen, aktivieren Sie die Option **Inherit properties from the Default group**.
4. Klicken Sie auf **OK**.

Konfigurieren von Ressourcen für eine Benutzergruppe

Ressourcen für Benutzergruppen werden im rechten Bereich der Registerkarte **Access Policy Manager** konfiguriert. Zu den Ressourcen gehören:

- Network Resources
- Application Policies
- Endpoint Resources (Endpunktressourcen)
- Endpoint Policies (Endpunktrichtlinien)

Nachdem Sie die Einstellungen konfiguriert haben, ziehen Sie die Ressourcenrichtlinie auf die Gruppe im linken Bereich. Beispiel: Sie haben eine Netzwerkressource konfiguriert und gespeichert, in der die Netzwerke angegeben sind, zu denen die Benutzer eine Verbindung herstellen können. Wenn Sie eine Gruppe von temporären Mitarbeitern haben, für die nur eingeschränkte Rechte gelten, ziehen Sie die Ressource auf diese Gruppe und legen Sie dann für die Gruppe fest, dass sie nicht die Einstellungen der Standardgruppe erben soll. Wenn Sie eine Endpunktrichtlinie erstellt haben, können Sie sie im linken Bereich unter **Pre-Authentication Policies** und **Endpoint Policies** einer Gruppe hinzufügen.

Sie können für jede Benutzergruppe eine Zugriffssteuerungsliste (ACL) erstellen, indem Sie wie unter "Bereitstellen von Netzwerkzugriff für Benutzer" auf Seite 112 beschrieben die Ressourcen festlegen, auf die die jeweilige Gruppe zugreifen darf. Die Zugriffssteuerungslisten werden für alle Gruppen, denen die Benutzer angehören, kombiniert und dann auf die Benutzer angewendet.

Sofern nicht alle Benutzer vollen Zugriff auf alle zugänglichen Netzwerke haben sollen, müssen Sie die Benutzergruppen mit Ressourcengruppen verknüpfen.

Konfigurieren von Benutzern, die mehreren Gruppen angehören

Wenn Benutzer Mitglied mehrerer Gruppen sind, werden einige Gruppeneinstellungen *vereint*. Dabei handelt es sich um folgende Einstellungen:

- Network Resources
- Application Policies
- Endpoint Policies (Endpunktrichtlinien)

Für die vereinten Einstellungen gelten folgende Ausnahmen:

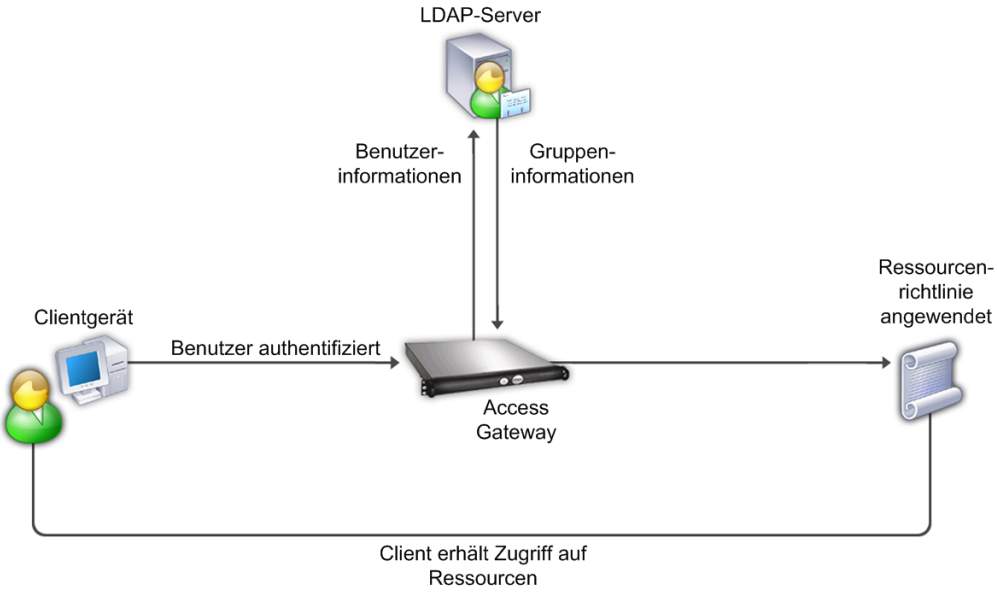
- Deny applications without policies: Wenn für eine der Gruppen, zu denen ein Benutzer gehört, die Option **Deny applications without policies** aktiviert ist, gilt diese Einstellung auch für den Benutzer.
- Enable IP pools: Die Benutzer übernehmen die IP-Adresse von der Gruppe mit der höchsten Priorität, für die IP-Pools aktiviert sind.
- Inherit properties from the Default Group: Wenn für eine der Gruppen, zu denen ein Benutzer gehört, die Option **Inherit properties from the Default Group** aktiviert ist, erbt der Benutzer die Einstellungen der Standardgruppe.

Die Einstellungen, die nicht vereint werden, richten sich nach der Gruppenpriorität. Dazu gehören folgende Einstellungen:

- Authenticate after network interruption/Authenticate upon system resume
- Enabling single sign-on with Windows
- Run logon scripts
- Session timeout
- Enable split DNS
- Access Gateway-Portalseiten

Konfigurieren von Netzwerkressourcen

Netzwerkressourcen definieren die Speicherorte in dem gesicherten Netzwerk, auf die autorisierte Benutzer zugreifen können. Ressourcengruppen sind mit Benutzergruppen verknüpft, um so Richtlinien für die Ressourcenzugriffssteuerung zu bilden.



Netzwerktopologie für Ressourcengruppen und Authentifizierung

Stellen Sie sich vor, Sie möchten einer Benutzergruppe den sicheren Zugriff auf Folgendes bereitstellen:

- Subnetz 10.10.x.x
- Subnetz 10.20.10.x
- IP-Adressen 10.50.0.60 und 10.60.0.10

Erstellen Sie zu diesem Zweck eine Netzwerkressourcengruppe, indem Sie das folgende Paar aus IP-Adresse und Subnetzmaske festlegen:

```
10.10.0.0/255.255.0.0
10.20.10.0/255.255.255.0
10.50.0.60/255.255.255.255
10.60.0.10/255.255.255.255
```

Die Subnetzmaske können Sie in der CIDR-Notation (Classless Inter Domain Routing) angeben. Beispiel: Sie könnten 10.60.0.10/32 als letzten Eintrag festlegen.

Beachten Sie beim Arbeiten mit Ressourcengruppen darüber hinaus die folgenden Hinweise.

- Sie können den Zugriff zusätzlich einschränken, indem Sie für ein Paar aus IP-Adresse und Subnetzmaske einen Port, einen Portbereich und ein Protokoll angeben. So könnten Sie z. B. festlegen, dass eine Ressource nur Port 80 und das TCP-Protokoll verwenden kann.
- Beim Konfigurieren des Ressourcengruppenzugriffs für eine Benutzergruppe können Sie den Zugriff auf jede Ressourcengruppe zulassen oder verweigern. Auf diese Weise können Sie einen Teil einer ansonsten zugelassenen Ressource ausschließen. So können Sie z. B. einer Benutzergruppe den Zugriff auf 10.20.10.0/24 erlauben, während Sie aber den Zugriff auf 10.20.10.30 verweigern. Verweigerungsregeln haben eine höhere Priorität als Zulassungsregeln.
- Die einfachste Methode, allen Benutzergruppen den Zugriff auf alle Netzwerkressourcen bereitzustellen, besteht darin, überhaupt keine Ressourcengruppen zu erstellen und die Option **Deny access without access control list (ACL)** auf der Registerkarte **Global Cluster Policies** zu deaktivieren. Alle Benutzergruppen haben dann Zugriff auf alle Netzwerkressourcen, auf die über das Access Gateway zugegriffen werden kann.
- Wenn Sie Benutzergruppen haben, die Zugriff auf alle Netzwerkressourcen benötigen, erstellen Sie eine Ressourcengruppe für 0.0.0.0/0.0.0.0 und geben Sie den Benutzergruppen Zugriff auf diese Ressource. Für alle anderen Benutzergruppen können Sie die einzelnen Ressourcengruppen nach Bedarf zulassen oder verweigern.

So erstellen und konfigurieren Sie eine Netzwerkressource

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Klicken Sie mit der rechten Maustaste im linken Bereich auf **Network Resources** und klicken Sie dann auf **New Network Resource**.
3. Geben Sie einen Namen für die Gruppe ein und klicken Sie auf **OK**.
4. Geben Sie unter **Network and subnet mask** das Paar aus IP-Adresse und Subnetzmaske für die Ressource in das Feld **Subnets** ein. Sie können für die Subnetzmaske die CIDR-Notation verwenden. Trennen Sie die einzelnen Einträge durch ein Leerzeichen voneinander.

5. Geben Sie unter **Port or port range** die Ports ein, über die das Access Gateway Verbindungen zu den Netzwerkressourcen herstellen kann. Sie haben folgende Optionen:

   - Geben Sie eine 0 (Null) ein, um alle Ports zu verwenden.
   - Geben Sie einen einzelnen Port ein oder mehrere Ports, die nicht in einem Bereich unmittelbar aufeinander folgen. Wenn Sie mehrere Ports eingeben, trennen Sie sie durch ein Komma. Beispiel: Wenn Sie Verbindungen über die Ports 22, 80 und 8088 zulassen möchten, geben Sie Folgendes ein:

     22, 80, 8080
   - Geben Sie einen Portbereich ein. Trennen Sie den ersten Port in der Reihenfolge mit einem Bindestrich (-) vom letzten Port des Bereichs. Beispiel: Wenn Sie Verbindungen über alle Ports von 110 bis 120 zulassen möchten, geben Sie Folgendes ein:

     110-120
   - Sie können auch eine Kombination aus einzelnen Ports und Portbereichen eingeben. Beispiel: Wenn Sie Verbindungen über die Ports 22, 80, 8088 und 110 bis 120 zulassen möchten, geben Sie Folgendes ein:

     22, 80, 8080, 110-120

6. Wählen Sie unter **Protocol** die Protokolle aus, mit denen Verbindungen auf den angegebenen Ports hergestellt werden können, und klicken Sie auf **OK**.

So fügen Sie einer Gruppe eine Netzwerkressource hinzu

Klicken Sie auf der Registerkarte **Access Policy Manager** im rechten Bereich unter **Network Resources** auf die Ressource, die Sie hinzufügen möchten, und ziehen Sie sie auf die Benutzergruppe im linken Bereich.

Zulassen und Verweigern von Netzwerkressourcen und Anwendungsrichtlinien

Standardmäßig sind alle Netzwerkressourcen und Anwendungsrichtlinien zugelassen. Wenn der Zugriff auf eine Ressourcengruppe verweigert wird, wird automatisch auch der Zugriff auf alle anderen Ressourcengruppen verweigert und der Netzwerkzugriff für die Benutzergruppe wird nur über deren Zugriffssteuerungsliste gesteuert.

Das Access Gateway interpretiert "Zulassen" und "Verweigern" wie folgt:

- Das Access Gateway verweigert den Zugriff auf alle Netzwerkressourcen oder Anwendungsrichtlinien, die nicht explizit zugelassen sind. Wenn Sie einer bestimmten Benutzergruppe also den Zugriff auf nur eine Ressourcengruppe erlauben möchten, gestatten Sie ihr auch nur den Zugriff auf diese bestimmte Ressourcengruppe.
- Verweigerungsregeln haben eine höhere Priorität als Zulassungsregeln. Auf diese Weise können Sie den Zugriff auf einen ganzen Bereich von Ressourcen erlauben, gleichzeitig aber auch den Zugriff auf ausgewählte Ressourcen innerhalb dieses Bereichs verweigern. Stellen Sie sich z. B. vor, Sie möchten einer Gruppe den Zugriff auf eine Ressourcengruppe im Bereich 10.20.10.0/24 erlauben, müssen dabei aber der Gruppe den Zugriff auf 10.20.10.30 verweigern. Um dies umzusetzen, müssen Sie zwei Ressourcengruppen erstellen: eine, die das Subnetz 10.20.10.0/24 enthält, und eine andere, die 10.20.10.30 enthält. Der Zugriff auf diese Ressource wird so lange verweigert, bis Sie ihn explizit erlauben.

So konfigurieren Sie die Ressourcenzugriffssteuerung für eine Gruppe

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Konfigurieren Sie im rechten Bereich die Gruppenressourcen.

   Wenn die Ressource konfiguriert ist, klicken Sie auf die Ressource und ziehen Sie sie auf die Gruppe im linken Bereich.
3. Wenn Sie den Zugriff auf eine Ressource zulassen oder verweigern möchten, klicken Sie mit der rechten Maustaste im linken Bereich auf die Netzwerkressource oder die Anwendungsrichtlinie und klicken Sie dann auf **Allow** oder **Deny**.

So entfernen Sie eine Ressource von einer Benutzergruppe

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Erweitern Sie im linken Bereich die Gruppe und dann den entsprechenden Richtlinien-Knoten.
3. Klicken Sie mit der rechten Maustaste auf die Ressource, die Sie entfernen möchten, und klicken Sie dann auf **Remove**.

Festlegen von Anwendungsrichtlinien

Anwendungsrichtlinien dienen dazu, den Netzwerkpfad einzuschränken, auf den Anwendungen zugreifen können. Angenommen, Benutzer verwenden für den E-Mail-Verkehr im Unternehmen Microsoft Outlook 2003. Sie können Outlook so konfigurieren, dass es einen bestimmten Netzwerkpfad zum Microsoft Exchange-Server verwendet. Wenn die Netzwerkressource definiert ist, sucht Outlook beim Starten nach der Netzwerkressource und der Endpunktrichtlinie (sofern definiert). Bei Erfolg können die Benutzer sich anmelden und E-Mails abrufen. Sonst startet Outlook nicht.

Wenn die Anwendung bereits vor der Verbindungherstellung zum Access Gateway geöffnet ist, bleibt sie geöffnet, aber die Richtlinien werden wirksam, sodass der Benutzer die Anwendung u. U. nicht mehr verwenden kann.

Wenn für eine Anwendung keine Netzwerkressource oder Endpunktrichtlinie konfiguriert ist und wenn auf der Registerkarte **General** das Kontrollkästchen **Deny applications without policies** aktiviert ist, wird der Anwendung der Zugriff auf das Netzwerk verweigert.

So konfigurieren Sie eine Anwendungsrichtlinie

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Klicken Sie mit der rechten Maustaste im rechten Bereich auf **Application Policies** und klicken Sie dann auf **New Application Policy**.
3. Geben Sie einen Namen für die Ressource ein und klicken Sie auf **OK**.
4. Geben Sie unter **Application** den Namen der Anwendung ein oder klicken Sie auf **Browse**, um zur Anwendung zu navigieren und sie auszuwählen.

   Im Feld **MD5** wird automatisch die Binärsumme der Anwendung eingetragen.

5. Wenn Sie die Anwendung auf bestimmte Netzwerke beschränken möchten oder eine Endpunktrichtlinie vorhanden sein muss, führen Sie unter **Application Policies** einen der folgenden Schritte aus:

   - Wenn Sie der Anwendungsrichtlinie eine Netzwerkressource hinzufügen möchten, klicken Sie im linken Bereich unter **Network Resources** auf die Ressource und ziehen Sie sie auf **Application network policies**.
   - Wenn Sie der Anwendungsrichtlinie eine Endpunktrichtlinie hinzufügen möchten, klicken Sie unter **End Point Policies** auf die Richtlinie und ziehen Sie sie auf **Application end point policies**.

6. Klicken Sie auf **OK**.

Durch Anwendungsrichtlinien wird der Netzwerkzugriff weiter eingeschränkt, indem einzelne Netzwerkressourcen bestimmten Anwendungen zugewiesen werden. Anwendungsrichtlinien definieren den Netzwerkpfad und die Endpunktrichtlinien für eine bestimmte Anwendung.

So fügen Sie einer Gruppe eine Anwendungsrichtlinie hinzu

1. Klicken Sie auf der Registerkarte **Access Policy Manager** im rechten Bereich unter **Application Policies** auf die Richtlinie, die Sie hinzufügen möchten, und ziehen Sie sie dann auf die Benutzergruppe im linken Bereich.
2. Klicken Sie zum Zulassen oder Verweigern des Zugriffs mit der rechten Maustaste auf die Anwendungsrichtlinie und klicken Sie dann auf **Allow** oder **Deny**.

Wenn eine Anwendungsrichtlinie erstellt und dann einer Benutzergruppe hinzugefügt wird, kann die Anwendung nur den festgelegten Netzwerkpfad und die angegebene Endpunktrichtlinie verwenden. Andere Anwendungen werden dadurch aber nicht an der Verwendung dieser Ressourcen gehindert. Wenn Anwendungen an der Verwendung dieser Netzwerkressourcen gehindert werden sollen, können Sie den Zugriff auf das Netzwerk verweigern.

So verweigern Sie den Netzwerkzugriff für Anwendungen ohne Richtlinien

1. Klicken Sie mit der rechten Maustaste auf der Registerkarte **Access Policy Manager** auf eine Benutzergruppe und klicken Sie dann auf **Properties**.
2. Aktivieren Sie auf der Registerkarte **General** unter **Application options** die Option **Deny applications without policies**.

Es ist möglich, einer Anwendung den Zugriff auf das Netzwerk zu verweigern, während alle anderen Anwendungen auf das Netzwerk zugreifen können.

So verweigern Sie einer Anwendung den Zugriff auf das Netzwerk

1. Klicken Sie mit der rechten Maustaste auf der Registerkarte **Access Policy Manager** auf eine Benutzergruppe und klicken Sie dann auf **Properties**.
2. Deaktivieren Sie auf der Registerkarte **General** unter **Application options** die Option **Deny applications without policies**.
3. Klicken Sie auf **OK** und schließen Sie das Dialogfeld **Properties**.
4. Klicken Sie mit der rechten Maustaste im rechten Bereich auf **Application Policies** und klicken Sie dann auf **New Application Policy**.
5. Geben Sie einen Namen für die Richtlinie ein und klicken Sie auf **OK**.
6. Geben Sie im Bereich **Application resource** unter **Application** den Anwendungsnamen ein oder klicken Sie auf **Browse**, um die Anwendung zu suchen und auszuwählen. Wenn dieses Feld ausgefüllt ist, wird das Feld **MD5** automatisch ausgefüllt.
7. Wenn Sie die Anwendung auf einen bestimmten Netzwerkpfad beschränken möchten, klicken Sie im linken Bereich unter **Network Resources** auf eine Netzwerkressource und ziehen Sie sie dann auf **Application network policies**.

   Andere konfigurierte Netzwerkressourcen müssen bereits einer Benutzergruppe zugeordnet sein und für sie muss die Option "Deny" festgelegt sein. Klicken Sie dazu im linken Bereich unter **Network Policies** in der Gruppe mit der rechten Maustaste auf die entsprechende Netzwerkressource und klicken Sie dann auf **Deny** und dann auf **OK**.
8. Klicken Sie auf die Anwendungsrichtlinie und ziehen Sie sie auf die Benutzergruppe, für die sie gilt.

Benutzer können Zugriff auf alle internen Netzwerke erhalten, die zugewiesen wurden. Der Anwendung wird der Zugriff auf das Netzwerk jedoch verweigert.

Sie können auch den Zugriff aller Anwendungen auf das Netzwerk verweigern, dabei aber den Zugriff auf einen bestimmten Netzwerkpfad zulassen, um so einen eingeschränkten Zugriff zu erzielen. Die Vorgehensweise ist mit der unter "So verweigern Sie einer Anwendung den Zugriff auf das Netzwerk" auf Seite 128 beschriebenen Vorgehensweise identisch. Der einzige Unterschied ist, dass die Option **Deny applications without policies** nicht deaktiviert, sondern aktiviert werden muss. Durch Aktivieren dieser Option wird der gesamte Anwendungszugriff auf das gesicherte Netzwerk verweigert. Wenn Sie einen Anwendungsnetzwerkzugriff zulassen möchten, konfigurieren Sie die Anwendungsrichtlinie so, dass die Anwendung akzeptiert wird. Führen Sie dazu die in der vorherigen Schrittanweisung genannten Schritte aus.

Die Benutzer erhalten nur mit der Anwendung, die explizit zugelassen wurde, Zugriff auf die interne Site. Allen anderen Anwendungen auf dem Clientgerät ist es nicht erlaubt, auf das interne Netzwerk zuzugreifen.

Konfigurieren von Endpunktrichtlinien und -ressourcen

Endpunktressourcen bieten eine weitere Sicherheitsebene, da die Computer, mit denen Benutzer Verbindungen zum Access Gateway herstellen können, bestimmte Kriterien erfüllen müssen. So können Sie z. B. festlegen, dass ein Computer bestimmte Registrierungseinträge, Dateien und/oder aktive Prozesse haben muss.

Jede Endpunktregel legt dabei fest, dass ein Computer über eines, mehrere oder alle der folgenden Merkmale verfügen muss:

- Einen Registrierungseintrag, mit einem von Ihnen festgelegten Pfad, Eintragstyp und Wert.
- Eine Datei, mit einem von Ihnen festgelegten Pfad, Dateinamen und Datum. Für die Datei kann auch eine Prüfsumme angegeben werden.
- Ein von Ihnen festgelegter ausgeführter Prozess. Für den Prozess kann auch eine Prüfsumme angegeben werden.

Endpunktrichtlinien werden auf die einzelnen Gruppen angewendet, indem ein boolescher Ausdruck festgelegt wird, in dem die Endpunkt-Ressourcennamen verwendet werden. Weitere Informationen hierzu finden Sie unter "Erstellen einer Endpunktrichtlinie für eine Gruppe" auf Seite 130.

So erstellen Sie eine Endpunktressource

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Klicken Sie mit der rechten Maustaste im rechten Bereich auf **End Point Resources** und klicken Sie dann auf **New End Point Resource**.
3. Geben Sie einen Namen ein und klicken Sie dann auf **OK**.

So erstellen Sie eine Prozessregel

1. Klicken Sie auf **Process rule**.
2. Geben Sie unter **Process name** den Namen des Prozesses ein oder klicken Sie auf **Browse**, um zu dem Prozess zu navigieren.

   Wenn ein Prozessname eingegeben ist, wird das Feld **MD5** automatisch ausgefüllt. Klicken Sie auf **OK**.

So erstellen Sie eine Dateiregel

1. Klicken Sie auf **File rule**.
2. Geben Sie unter **File name** den Pfad und den Dateinamen ein oder klicken Sie auf **Browse**, um zu der Datei zu navigieren.

   Wenn ein Dateiname eingegeben wurde, wird das Feld **MD5** automatisch ausgefüllt.
3. Geben Sie unter **Date** das Datum ein. Verwenden Sie dazu das folgende Format: MM/TT/JJJJ. Dies ist das Datum, an dem die Datei erstellt wurde. Klicken Sie auf **OK**.

So erstellen Sie eine Registrierungsregel

1. Klicken Sie auf **Registry rule**.
2. Geben Sie unter **Registry path** den Pfad ein und wählen Sie einen Schlüsseltyp aus.
3. Geben Sie unter **Registry entry** den Schlüsselnamen ein.
4. Geben Sie unter **Registry value** den Wert ein, auf den der Schlüssel gesetzt werden muss, und klicken Sie auf **OK**.

So löschen Sie eine Endpunktressource

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Klicken Sie mit der rechten Maustaste im rechten Bereich auf die Endpunktressource, die entfernt werden soll, und klicken Sie dann auf **Remove**.

Erstellen einer Endpunktrichtlinie für eine Gruppe

Sie können einen booleschen Ausdruck erstellen, indem Sie Endpunktressourcen auf den End Point Policy Expression Generator ziehen und dort ablegen. Der Generator erstellt den Ausdruck automatisch, wenn Sie die Ressourcen per Drag & Drop in den Generator ziehen. Ausdrücke können jederzeit bearbeitet werden.

Geben Sie zum Konfigurieren einer Endpunktrichtlinie für eine Gruppe einen Ausdruck an, der die Endpunktressourcen enthält, die auf die Gruppe angewendet werden sollen.

Angenommen, Sie erstellen die folgenden Endpunktrichtlinien:

UntRessRegEintrag

AntiVirusProzess1

AntiVirusProzess2

Ihr Endpunktrichtlinienausdruck könnte festlegen, dass eine Registrierungsprüfsumme verifizieren muss, dass die Ressource, die versucht, eine Verbindung herzustellen, zum Unternehmen gehört und dass auf der Ressource einer der Antivirusprozesse ausgeführt werden muss. Ein solcher boolescher Ausdruck würde wie folgt aussehen:

```
(UntRessRegEintrag & (AntiVirusProzess1 | AntiVirusProzess2))
```

Gültige Operatoren für Endpunktrichtlinienausdrücke:

( )	dient zum Verschachteln von Ausdrücken, um deren Auswertung zu steuern
&	logisches UND
|	logisches ODER
!	logisches NICHT

Bei Benutzern ohne Administratorrechte schlagen die Endpunktrichtlinien fehl, wenn die Richtlinie eine Datei in einer eingeschränkten Zone (wie z. B. C:\Dokumente und Einstellungen\Administrator) oder einen eingeschränkten Registrierungsschlüssel enthält.

Wenn ein Benutzer mehreren Gruppen angehört, besteht die für den Benutzer geltende Endpunktrichtlinie aus der Kombination der Ausdrücke für die einzelnen Gruppen des Benutzers.

So konfigurieren Sie eine Endpunktrichtlinie für eine Gruppe

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Klicken Sie mit der rechten Maustaste im rechten Bereich auf **End Point Policies** und klicken Sie dann auf **New End Point Policy**.
3. Geben Sie einen Namen ein und klicken Sie auf **OK**.

Nachdem die Richtlinie erstellt wurde, ziehen Sie die Endpunktressourcen per Drag & Drop auf den Expression Builder, um den Ausdruck zu erhalten.

So konstruieren Sie einen Endpunktrichtlinienausdruck

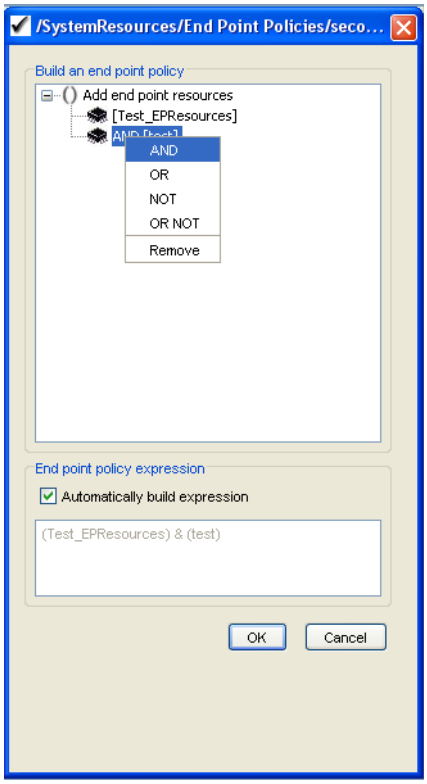
1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Klicken Sie mit der rechten Maustaste im rechten Bereich auf eine Endpunktrichtlinie und klicken Sie auf **Properties**.

   Die Eigenschaftenseite wird geöffnet und der Ressourcenbereich wird nach links verschoben.
3. Klicken Sie unter **End point policy expression** auf **Automatically build expression**.
4. Ziehen Sie eine Ressource in den Bereich **Build an end point policy** (im oberen Bereich des Dialogfelds) und legen Sie sie auf **Add end point resources**.
5. Der Ausdruck wird mit **AND** erstellt. Wenn Sie dies ändern möchten, klicken Sie mit der rechten Maustaste auf eine der Ressourcen und wählen Sie im Menü eine andere Option aus. Klicken Sie auf **OK**.

Der Endpunktrichtlinienausdruck wird automatisch konfiguriert. Wenn Sie den Ausdruck manuell bearbeiten möchten, deaktivieren Sie die Option **Automatically build expression**. Citrix empfiehlt jedoch, die Option aktiviert zu lassen, um Fehler im Ausdruck zu vermeiden.

Ändern des Endpunktrichtlinienoperators

Beim Zusammenstellen eines Ausdrucks für eine Endpunktrichtlinie ist der Operator automatisch AND. Sie ändern den Operator, indem Sie mit der rechten Maustaste auf die Endpunktressource klicken und den gewünschten Operator auswählen:



Erstellen eines Endpunktrichtlinienausdrucks

Festlegen der Priorität von Gruppen

Bei Benutzern, die mehreren Gruppen angehören, können Sie über die Gruppenpriorität bestimmen, welche Richtlinien für den Benutzer gelten sollen. Angenommen, einige Benutzer gehören sowohl zur Gruppe "Vertrieb" als auch zur Gruppe "Support". Wenn die Gruppe "Vertrieb" in der Liste "User Groups" vor der Gruppe "Support" steht, gelten für die Benutzer, die beiden Gruppen angehören, die Richtlinien der Gruppe "Vertrieb". Steht die Gruppe "Support" in der Liste vor der Gruppe "Vertrieb", gelten die Richtlinien der Gruppe "Support".

Die Gruppenpriorität wirkt sich auf die folgenden Richtlinien aus:

- Portalseitenkonfiguration: Hiermit wird festgelegt, welche Portalseite Benutzer beim Herstellen einer Verbindung sehen. Die Portalseite kann die Vorlage sein, die im Access Gateway enthalten ist, oder sie kann auf das Webinterface verweisen.
- Benutzertimeouts: Hiermit wird festgelegt, wie lange eine Sitzung aktiv sein kann. Es gibt folgende Timeouts:
    - Sitzungstimeouts, bei denen eine Verbindung nach einer festgelegten Zeitspanne geschlossen wird.
    - Netzwerkaktivitätstimeouts, wobei das Access Gateway Plug-in während eines festgelegten Zeitraums keinen Netzwerkverkehr feststellt.
    - Timeout bei inaktiven Sitzungen, wobei das Access Gateway Plug-in während eines festgelegten Zeitraums keine Maus- oder Tastaturaktivität feststellt.
- Aktivieren von Split DNS: Hiermit wird das Failover auf das lokale DNS des Benutzers ermöglicht.
- Benutzerneuanmeldung nach einem Netzwerkausfall oder wenn der Computer aus dem Ruhezustand oder dem Standby-Modus aktiviert wird.

Das Access Gateway berücksichtigt alle Benutzergruppen. Wenn Benutzer Mitglied von mehreren Gruppen sind und das Kontrollkästchen **Deny applications without policies** für eine der Gruppen aktiviert ist, werden die Benutzeranwendungen verweigert, unabhängig davon, welche Einstellungen für andere Gruppen gelten.

Wenn Benutzer Mitglied in mehreren Gruppen sind und IP-Pooling in einer dieser Gruppen aktiviert ist, weist das Access Gateway eine IP-Adresse aus dem Pool der ersten Gruppe zu, in der IP-Pooling aktiviert ist.

Gruppen werden zunächst in der Reihenfolge aufgeführt, in der sie erstellt wurden.

So legen Sie die Priorität von Gruppen fest

1. Klicken Sie auf die Registerkarte **Group Priority**.
2. Wählen Sie eine Gruppe aus, die verschoben werden soll, und verschieben Sie die Gruppe mit den Pfeilschaltflächen in der Liste nach oben oder unten.

   Die Gruppe, die in der Liste ganz oben steht, hat die höchste Priorität.

Konfigurieren von Vorauthentifizierungsrichtlinien

Mit Vorauthentifizierungsrichtlinien können Benutzer vom Anmelden am Access Gateway ausgeschlossen werden. Wenn Benutzer für die Verbindung zum Access Gateway einen Webbrowser verwenden, scannt die Vorauthentifizierungsrichtlinie das Clientgerät, bevor das Anmeldedialogfeld angezeigt wird. Wenn der Scan fehlschlägt, können sich die Benutzer nicht anmelden. Zum Anmelden am Webportal müssen Benutzer die richtigen Anwendungen installieren.

So erstellen Sie Vorauthentifizierungsrichtlinien

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Wählen Sie unter **End Point Policies** die konfigurierte Richtlinie aus und ziehen Sie sie in den linken Bereich auf **Pre-Authentication Policies** (unter dem Richtlinienknoten **Global Policies**).

Informationen zum Erstellen und Konfigurieren von Endpunktressourcen und -richtlinien finden Sie unter "Konfigurieren von Endpunktrichtlinien und -ressourcen" auf Seite 129.

Konfigurieren des Access Gateways für Citrix Branch Repeater

Das Access Gateway kann mit Citrix Branch Repeater verwendet werden, um die Anwendungsbeschleunigung zu unterstützen. Citrix Branch Repeater verbessert CIFS- (Common Internet File System) und HTTP-Verbindungen und beschleunigt den Datenverkehr über das Access Gateway. Das Access Gateway wird in der DMZ installiert und das Citrix Branch Repeater-Gerät wird hinter dem Access Gateway im gesicherten Netzwerk platziert. Benutzer verbinden sich über das Access Gateway und Citrix Branch Repeater mit Ressourcen im gesicherten Netzwerk.

Zwei Einstellungen müssen konfiguriert werden, um die Citrix Branch Repeater-Beschleunigung zu unterstützen:

- Beständigkeit der TCP-Optionen für jedes Netzwerk, das auf dem Access Gateway konfiguriert ist. Sie konfigurieren Netzwerkressourcen und wenden dann die Richtlinie für jedes Netzwerk an, auf dem die TCP-Einstellungen erhalten bleiben sollen.
- Konfigurieren des Access Gateways für die Kommunikation mit dem Citrix Repeater Plug-in. Wenn dies konfiguriert ist, sendet das Access Gateway eine Filterliste and das Repeater Plug-in mit den Einstellungen für die Citrix Branch Repeater-Optimierung.

So konfigurieren Sie die TCP-Optimierung auf dem Access Gateway

1. Klicken Sie im Administration Tool auf die Registerkarte **Global Cluster Policies**.
2. Wählen Sie unter **Advanced options** die Option **Enable application acceleration with the Accelerator Plugin** und klicken Sie auf **Submit**.
3. Doppelklicken Sie auf der Registerkarte **Access Policy Manager** auf der rechten Seite unter **Network Resources** auf eine konfigurierte Netzwerkressource oder erstellen Sie eine neue Ressource.
4. Wählen Sie **Preserve TCP options** und klicken Sie auf **OK**.
5. Ziehen Sie die Netzwerkrichtlinie auf die Benutzergruppe, für die die Richtlinie gelten soll.

Konfigurieren von Benutzerverbindungen für das Citrix Access Gateway Plug-in

In diesem Kapitel werden Benutzerverbindungen besprochen sowie die Methoden, mit denen Benutzer Verbindungen zum Access Gateway und zu internen Ressourcen mit dem Citrix Access Gateway Plug-in herstellen können.

Benutzerverbindungen werden mit sicheren Verbindungen wie folgt aufgebaut:

- Über einen Webbrowser, der eine Verbindung zum Access Gateway herstellt
- Über das Access Gateway Plug-in, das auf dem Clientgerät installiert ist

Bei der Verbindungsherstellung wird ein sicherer Tunnel zum gesicherten Netzwerk gebildet und das Access Gateway übernimmt den SSL-Handshake.

Dieses Kapitel enthält:

- "Systemvoraussetzungen"
- "Funktionsweise von Benutzerverbindungen"
- "Unterstützen des Access Gateway Plug-ins"
- "Konfigurieren von Proxyservern für das Access Gateway Plug-in"
- "Installieren des Access Gateway Plug-ins mit dem MSI-Paket"
- "Konfigurieren von Single Sign-on für Windows-Betriebssysteme"
- "Verbinden mit früheren Versionen des Access Gateway Plug-ins"
- "Herstellen einer Verbindung mit einer Webadresse"
- "Anmelden mit dem Access Gateway Plug-in"
- "Installieren des Access Gateway Plug-ins für Linux"

- "Konfigurieren der Authentizierungsanforderungen nach einer Netzwerkunterbrechung"
- "Konfigurieren weiterer Gruppeneigenschaften"
- "Anfordern von Clientzertifikaten für die Authentifizierung"
- "Installieren von Stammzertifikaten"
- "Auswählen einer Verschlüsselungsart für Clientverbindungen"

Systemvoraussetzungen

Das Access Gateway Plug-in wird von folgenden Betriebssystemen und Webbrowsern unterstützt.

Betriebssysteme

Das Access Gateway Plug-in wird auf folgenden Windows-Betriebssystemen unterstützt:

- Windows XP Home Edition
- Windows XP Professional
- Windows 2000 Server
- Windows Server 2003
- Windows Vista (32 Bit)

Webbrowser

Das Access Gateway Plug-in wird von folgenden Webbrowsern unterstützt:

- Microsoft Internet Explorer, Versionen 6.*x* und 7.*x*
- Mozilla Firefox Version 1.5 und höher

Funktionsweise von Benutzerverbindungen

Das Access Gateway funktioniert folgendermaßen:

- Wenn Benutzer sich zum ersten Mal über eine Webadresse verbinden, melden sie sich an und wählen dann das Access Gateway Plug-in aus, das heruntergeladen und auf dem Clientgerät installiert wird.
- Nachdem das Access Gateway Plug-in heruntergeladen und installiert wurde, melden sich Benutzer noch einmal an. Wenn die Authentifizierung erfolgreich war, richtet das Access Gateway einen sicheren Tunnel ein. Ist das Access Gateway Plug-in bereits auf dem Clientgerät installiert und Benutzer melden sich über die Webadresse an, prüft das Access Gateway Plug-in, ob Updates vorliegen und dann werden die Benutzer angemeldet.
- Sobald Remotebenutzer versuchen, über das Gerät auf die Netzwerkressourcen zuzugreifen, verschlüsselt das Access Gateway Plug-in den gesamten Netzwerkverkehr, der für das interne Netzwerk der Organisation bestimmt ist, und leitet die Pakete an das Access Gateway weiter.
- Das Access Gateway fungiert als Endpunkt des SSL-Tunnels (terminiert den Tunnel), akzeptiert den eingehenden Verkehr, der für das private Netzwerk bestimmt ist, und leitet den Verkehr an das private Netzwerk weiter. Das Access Gateway sendet den Verkehr über einen sicheren Tunnel zum Clientgerät zurück.

Wenn Benutzer sich mit dem Access Gateway Plug-in anmelden, werden sie vom Access Gateway aufgefordert, sich zu authentifizieren. Das Access Gateway authentifiziert die Anmeldeinformationen mit einem Authentifizierungsverfahren, z. B. mit der lokalen Authentifizierung, RSASecurID, SafeWord, LDAP, NTLM oder RADIUS. Wenn die Anmeldeinformationen korrekt sind, schließt das Access Gateway den Handshake mit dem Plug-in ab. Dieser Anmeldeschritt ist nur dann erforderlich, wenn Benutzer das Secure Access Plug-in zum ersten Mal herunterladen.

Wenn Benutzer hinter einem Proxyserver sind, können sie den Proxyserver und die Authentifizierungsinformationen angeben. Weitere Informationen hierzu finden Sie unter "Konfigurieren von Proxyservern für das Access Gateway Plug-in" auf Seite 144.

Das Secure Access Plug-in wird auf dem Clientgerät installiert. Nach der ersten Verbindung können Benutzer sich mit einem Webbrowser oder über das Startmenü anmelden.

Das Dialogfeld **Citrix Access Gateway - Optionen** in dem Sie Clientgeräteinstellungen machen, kann auch über das Startmenü geöffnet werden oder indem Sie im Anmeldedialogfeld mit der rechten Maustaste klicken.

So öffnen Sie das Optionen-Dialogfeld über das Startmenü

Klicken Sie auf **Start > Alle Programme > Citrix > Citrix Access Clients > Citrix Access Gateway - Eigenschaften**.

Einrichten des sicheren Tunnels

Nachdem das Secure Access Plug-in gestartet wurde, richtet es einen sicheren Tunnel über den Port 443 (oder jeden anderen konfigurierten Port des Access Gateways) ein und sendet Authentifizierungsinformationen. Nachdem der Tunnel eingerichtet wurde, sendet das Access Gateway Konfigurationsinformationen an das Secure Access Plug-in, in denen beschrieben wird, welche Netzwerke gesichert werden sollen. Außerdem enthalten diese Informationen eine IP-Adresse, sofern IP-Pooling aktiviert wurde. Weitere Informationen über IP-Pooling finden Sie unter "Aktivieren von IP-Pooling" auf Seite 159.

Tunneln des privaten Netzwerkverkehrs über sichere Verbindungen

Sobald das Access Gateway Plug-in gestartet und Benutzer authentifiziert wurden, wird der gesamte Netzwerkverkehr, der für die angegebenen privaten Netzwerke bestimmt ist, über den sicheren Tunnel an das Access Gateway weitergeleitet.

Das Access Gateway fängt alle vom Clientgerät hergestellten Netzwerkverbindungen ab und multiplext/tunnelt diese über SSL an das Access Gateway, wo der Verkehr demultiplext wird und die Verbindungen an die korrekte Kombination aus Host und Port weitergeleitet werden.

Die Verbindungen unterliegen administrativen Sicherheitsrichtlinien für einzelne Anwendungen, einen Teilsatz von Anwendungen oder das gesamte Intranet. Sie legen die Ressourcen fest (Paare aus IP-Adressbereichen/Subnetzmasken), auf die die Remotebenutzer über die VPN-Verbindung zugreifen können. Weitere Informationen hierzu finden Sie unter "Konfigurieren von Netzwerkzugriff und Gruppenressourcen" auf Seite 111.

Alle IP-Pakete, gleich welchen Protokolls, werden abgefangen und über eine sichere Verbindung weitergeleitet. Von lokalen Anwendungen auf dem Clientgerät ausgehender Verkehr wird sicher durch den Tunnel zum Access Gateway geleitet, der dann die Verbindungen mit dem Zielserver wiederherstellt. Für die Zielserver sehen die Verbindungen so aus, als stammten sie vom lokalen Access Gateway im privaten Netzwerk, sodass die IP-Adresse des Clientgeräts verborgen wird. Dieses Verfahren wird auch *Reverse NAT* (Network Address Translation) genannt. Das Verbergen der IP-Adressen erhöht die Sicherheit der Standorte, von denen der Verkehr ausgeht.

Lokal, also auf dem Clientgerät, wird der gesamte verbindungsspezifische Verkehr (wie SYN-ACK-, PUSH-, ACK- und FIN-Pakete) vom Secure Access Plug-in neu erstellt, damit es so aussieht, als käme er vom privaten Server.

Funktionsweise bei Verwendung von Firewalls und Proxyservern

Unter Umständen sind Benutzer des Secure Access Plug-ins hinter der Firewall einer anderen Organisation, wie in der folgenden Abbildung dargestellt.

Clientverbindung durch zweite interne Firewalls.

NAT-Firewalls verfügen über eine Tabelle, mit deren Hilfe sie sichere Pakete vom Access Gateway zum Clientgerät zurücksenden können. Für schaltungsorientierte Verbindungen unterhält das Access Gateway eine portzugeordnete Reverse-NAT-Übersetzungstabelle. Die Reverse-NAT-Übersetzungstabelle versetzt das Access Gateway in die Lage, Verbindungen zuzuordnen und Pakete mit den richtigen Portnummern über den Tunnel zurück an das Clientgerät zu senden, sodass die Pakete zur korrekten Anwendung zurückkehren.

Der Access Gateway-Tunnel wird mit Industriestandardmethoden für Verbindungen hergestellt, wie HTTPS, Proxy HTTPS und SOCKS. Auf diese Weise wird sichergestellt, dass das Access Gateway firewall-zugänglich ist und Remotecomputer können auf private Netzwerke hinter der Firewall anderer Unternehmen zugreifen, ohne dass es dabei zu Problemen kommt.

So kann die Verbindung beispielsweise über einen Zwischenproxy, wie einen HTTP-Proxy, hergestellt werden, indem ein CONNECT HTTPS-Befehl an den Zwischenproxy gesendet wird. Alle Anmeldeinformationen, die der Zwischenproxy benötigt, werden wiederum vom Remotebenutzer bezogen (über die Single Sign-On-Informationen oder eine Aufforderung zur Eingabe der entsprechenden Informationen) und dann dem Zwischenproxyserver bereitgestellt. Nachdem die HTTPS-Sitzung eingerichtet wurde, wird der eigentliche Datenverkehr verschlüsselt und in Form von sicheren Paketen an das Access Gateway gesendet.

Beenden des sicheren Tunnels und Zurücksenden von Paketen an den Client

Das Access Gateway beendet den SSL-Tunnel und akzeptiert eingehende Pakete, die für das private Netzwerk bestimmt sind. Wenn die Pakete die Autorisierungs- und Zugriffssteuerungskriterien erfüllen, erzeugt das Access Gateway die IP-Header der Pakete neu, sodass sie aussehen, als stammten sie aus dem IP-Adressbereich des privaten Netzwerks, in dem das Access Gateway ist, oder von der vom Client zugewiesenen privaten IP-Adresse. Das Access Gateway sendet die Pakete dann an das Netzwerk.

Das Secure Access Plug-in unterhält zwei Tunnel: einen SSL-Tunnel über den Daten an das Access Gateway gesendet werden und einen Tunnel zwischen dem Clientgerät und lokalen Anwendungen. Die verschlüsselten Daten, die über den SSL-Tunnel ankommen, werden dann entschlüsselt, bevor sie über den zweiten Tunnel an die lokale Anwendung gesendet werden.

Wenn Sie eine Packet Sniffer wie Ethereal auf dem Clientgerät verwenden, auf dem das Secure Access Plug-in ausgeführt wird, sehen Sie unverschlüsselten Datenverkehr, der scheinbar zwischen dem Clientgerät und dem Access Gateway stattfindet. Dieser unverschlüsselte Verkehr läuft jedoch nicht über den Tunnel zwischen dem Client und dem Access Gateway, sondern über den Tunnel zu den lokalen Anwendungen.

Wenn ein Anwendungsclient eine Verbindung mit seinem Anwendungsserver herstellt, kann es vorkommen, dass bestimmte Protokolle verlangen, dass der Anwendungsserver im Gegenzug versucht, eine neue Verbindung mit dem Client herzustellen. In diesem Fall sendet der Client mittels eines individuellen Client-Server-Protokolls seine bekannte lokale IP-Adresse an den Server. Für diese Anwendungen präsentiert das Secure Access Plug-in der lokalen Clientanwendung eine private IP-Adresse, die das Access Gateway im internen Netzwerk verwendet. Dieses Feature wird von vielen Echtzeit-Sprachanwendungen und von FTP verwendet.

Benutzer können auf die Ressourcen im gesicherten Netzwerk zugreifen, indem sie über das Access Gateway eine Verbindung von ihrem eigenen Computer oder von einem öffentlichen Computer aus herstellen.

Unterstützen des Access Gateway Plug-ins

Damit die Benutzer eine Verbindung zum Access Gateway herstellen und es verwenden können, müssen Sie die folgenden Informationen bereitstellen:

- Webadresse für das Access Gateway (z. B. https://*AccessGatewayFQDN*/).
- Für die Anmeldung erforderlicher Name des Authentifizierungsbereichs (sofern Sie nicht den Bereich Default verwenden).
- Pfad zu allen Netzlaufwerken, auf die die Benutzer zugreifen können sollen; erfolgt durch Zuordnen eines Netzlaufwerks auf dem Clientgerät.
- Sämtliche Systemvoraussetzungen für das Ausführen des Access Gateway Plug-ins, sofern Endpunktressourcen und -richtlinien konfiguriert wurden.

Anhängig von der Konfiguration des Clientgeräts müssen Sie möglicherweise auch weitere Informationen angeben:

- Um das Secure Access Plug-in zu starten, müssen Windows XP-Benutzer lokale Administratoren oder Mitglied der Administratorengruppe sein, um das Access Gateway Plug-in beim ersten Start zu installieren. Für Upgrades müssen Benutzer nicht Administrator sein.
- Wenn auf dem Clientgerät eine Firewall installiert und aktiviert ist, müssen Benutzer u. U. die Firewalleinstellungen ändern, sodass der Verkehr zu oder von den IP-Adressen der Ressourcen nicht blockiert wird. Das Secure Access Plug-in kann automatisch Internetverbindungsfirewall in Windows XP und Windows-Firewall in Windows XP Service Pack 2 und Windows Vista einstellen. Weitere Informationen zum Konfigurieren verschiedener gängiger Firewalls finden Sie unter "Konfigurieren persönlicher Firewalls von Drittanbietern" auf Seite 196.
- Benutzer, die die Access Gateway-Verbindung für FTP verwenden möchten, müssen ihre FTP-Anwendung so einrichten, dass sie passive Übertragungen unterstützt. Eine passive Übertragung bedeutet, dass das Clientgerät die Datenverbindung zu Ihrem FTP-Server und nicht Ihr FTP-Server die Datenverbindung zum Remotecomputer einrichtet.

Da die Benutzer mit den Dateien und Anwendungen arbeiten, als wären sie lokal im Netzwerk der Organisation, ist keine Schulung der Benutzer und keine Konfiguration der Anwendungen nötig.

Es gibt eine E-Mail-Vorlage mit den in diesem Abschnitt besprochenen Informationen. Die Vorlage ist auf der Downloads-Seite des Administration Portals. Citrix empfiehlt, den Text für Ihre Site anzupassen und die E-Mail dann an die Benutzer zu senden.

Konfigurieren von Proxyservern für das Access Gateway Plug-in

Wenn das Access Gateway Plug-in die Verbindung herstellt, bevor die Richtlinien vom Access Gateway heruntergeladen werden, fragt das Plug-in Clientproxyeinstellungen vom Betriebssystem ab. Wenn die automatische Erkennung aktiviert ist, ändert das Access Gateway Plug-in automatisch die Clientproxyeinstellungen zu denen des Betriebssystems. Das Access Gateway Plug-in versucht, eine Verbindung zum Access Gateway herzustellen, die Vorauthentifizierungsrichtlinien herunter zu laden und fordert dann die Benutzer auf, die Anmeldeinformationen einzugeben. Wenn das Access Gateway Plug-in die Clientproxyeinstellungen nicht automatisch erkennen kann, wird eine direkte Verbindung ohne Proxyserver hergestellt. Die automatische Erkennung der Proxyeinstellungen wird im Access Gateway Plug-in im Optionen-Dialogfeld konfiguriert.

Während der Installation wird auf dem Clientgerät eine Installationsprotokolldatei CAG_Plug-in.log im Verzeichnis %TEMP% angelegt. Verwenden Sie diese Protokolldatei bei der Problembehandlung von Installationsproblemen.

Benutzer können einen Proxyserver auch manuell über das Access Gateway Plug-in konfigurieren. Wird ein Proxyserver manuell konfiguriert, wird dadurch die automatische Erkennung der Proxyeinstellungen deaktiviert.

So konfigurieren Sie einen Proxyserver manuell

1. Klicken Sie auf dem Clientgerät auf **Start > Alle Programme > Citrix > Citrix Access Clients > Citrix Access Gateway - Eigenschaften**.
2. Aktivieren Sie im Dialogfeld **Citrix Access Gateway-Optionen** unter **Proxyeinstellungen** die Option **Proxyserver manuell konfigurieren**.
3. Geben Sie in den Feldern **IP-Adresse** und **Port** die IP-Adresse und die Portnummer ein.
4. Wenn der Server eine Authentifizierung erfordert, wählen Sie **Proxyserver erfordert Authentifizierung**.

Installieren des Access Gateway Plug-ins mit dem MSI-Paket

Sie können das Access Gateway Plug-in auf dem Clientgerät mit einem MSI-Paket installieren. Das Access Gateway Plug-in wird pro Computer installiert. Beim Erstellen des Pakets können Sie festlegen, dass die Installation mit erhöhten Privilegien ausgeführt wird, sodass Benutzer ohne Administratorrechte das Plug-in installieren können.

Sie können das Paket erstellen, indem Sie die Datei CitrixAGP.exe vom Access Gateway-Gerät herunterladen. Wenn die ausführbare Datei heruntergeladen wurde, können Sie sie ausführen, um die MSI-Datei zu entpacken und zu installieren.

So laden Sie das MSI-Paket herunter und installieren es

1. Gehen Sie in einem Webbrowser zu https://*AccessGatewayFQDN*, wobei *AccessGatewayFQDN* der vollqualifizierte Domänenname (FQDN) des Access Gateways ist.
2. Klicken Sie auf **Speichern**, um die Datei auf Ihrem Computer zu speichern.
3. Doppelklicken Sie auf CitrixAGP.exe, um die MSI-Datei zu entpacken und zu installieren.

Es gibt zwei Methoden die MSI-Datei an Benutzer zu verteilen, die auf dem Clientgerät keine Administratoren sind:

- Verwenden Sie eine Active Directory-Gruppenrichtlinie (oder ein ähnliches Tool) für eine Push-Installation des Pakets auf das Clientgerät
- Kündigen Sie das Installationspaket auf dem Clientgerät an

Installation des MSI-Pakets mit einer Gruppenrichtlinie

Wenn Benutzer sich von einem internen Netzwerk mit Active Directory verbinden, können Sie das Access Gateway Plug-in mit einer Gruppenrichtlinie herunterladen und installieren. Die Softwareinstallationsfunktion der Gruppenrichtlinie installiert oder aktualisiert das Access Gateway Plug-in automatisch, wenn das Clientgerät eine Verbindung zur Domäne herstellt.

Die Installation des MSI-Pakets über eine Gruppenrichtlinie und das Ankündigen des Pakets sind ähnliche Vorgänge. Das Paket CitrixAGP.exe sollte extrahiert werden. Wenn die Standardkonfiguration der Installation geändert werden muss, führen Sie die administrative Installation aus und erstellen ein administratives Image. Kopieren Sie entweder die Original-MSI-Datei oder das administrative Image auf eine Netzwerkfreigabe. Weisen Sie das Paket mit einer Gruppenlinie Computern zu und verweisen Sie dabei auf die Netzwerkfreigabe.

So stellen Sie Access Gateway Plug-in mit einer Gruppenrichtlinie bereit

1. Erstellen Sie auf dem Windows-Server ein temporäres Verzeichnis und öffnen Sie es.
2. Wählen Sie auf dem Access Gateway-Gerät im Administration Tool auf der Registerkarte **Global Cluster Policies** unter **Access options** die Option **Do not upgrade earlier versions of the Access Gateway Plugin**
3. Geben Sie an der Eingabeaufforderung **CitrixAGP -extract** ein, um die MSI-Datei und zugehörige Dateien in das im 1. Schritt erstellte Verzeichnis zu extrahieren.
4. Veröffentlichen Sie die MSI-Datei und andere Dateien mit der Gruppenrichtlinie.

Installieren des MSI-Pakets durch Ankündigen

Um die Clientinstallation anzukündigen, müssen Sie die CAGSE.MSI- und MST-Dateien extrahieren. Beim Erstellen des Images müssen Sie einen Pfad zum Image sowie die Sprache angeben. Sie werden dann einen Befehlszeilenschalter für das MSIEXEC-Dienstprogramm, um das Paket anzukündigen.

Nur der angekündigte Dateipfad gilt für Windows Installer als vertrauenswürdig. Wenn Benutzer CAGSE.MSI von einer CD oder einem lokalen Pfad installieren, der sich von dem angekündigten Pfad unterscheidet, schlägt die Installation fehl.

So extrahieren Sie die MSI- und MST-Dateien und erstellen ein administratives Image

1. Wählen Sie im Administration Tool auf der Registerkarte **Global Cluster Policies** unter **Access options** die Option **Do not upgrade earlier versions of the Access Gateway Plugin**
2. Geben Sie an der Eingabeaufforderung Folgendes ein:

   CitrixAGP -extract

   Mit diesem Befehl werden die Dateien in der Freigabe extrahiert, die Sie angegeben haben. Geben Sie **CitrixAGP** ein, um das Access Gateway Plug-in zu extrahieren und zu installieren.
3. Um ein konfiguriertes administratives Image zu erstellen, geben Sie an der Eingabeaufforderung Folgendes ein:

   msiexec /a CAGSE.MSI
4. Wenn das Image erstellt ist, kündigen Sie das Produkt allen Benutzern des Clientgeräts an. Geben Sie dafür an einer Eingabeaufforderung auf dem Clientgerät Folgendes ein:

   misexec /jm *Pfad zu administrativem Image*\CAGSE.MSI

   Dieser Befehl kündigt das Access Gateway Plug-in an, installiert es aber nicht auf dem Clientgerät. Das Plug-in scheint installiert zu sein. In der Systemsteuerung und im Startmenü sind Einträge vorhanden, es wurden aber keine Dateien auf das Clientgerät kopiert.
5. Um das Access Gateway Plug-in zu installieren, geben Sie an einer Eingabeaufforderung Folgendes ein:

   msiexec /i *Pfad zu administrativem Image*\CAGSE.MSI

   Sie können die Installation auf durch Aufrufen der Startmenüverknüpfung starten.

Die Erstinstallation des Access Gateway Plug-ins auf dem Clientgerät wird mit dieser Methode durchgeführt.

Wenn ein Upgrade für das Plug-in verfügbar ist, aktualisieren Sie das Paket auf der Dateifreigabe. Wenn Benutzer sich mit dem Access Gateway verbinden, navigieren sie zu der Freigabe und führen cagsetup.exe aus, um das Upgrade zu erhalten.

Wenn das Access Gateway Plug-in Anmeldeskripte ausführt, kann mit dem Skript geprüft werden, ob Upgrades vorhanden sind und das Plug-in ggf. installiert werden. Sie können auch den Benutzern eine E-Mail schicken, dass das Upgrade verfügbar ist und einen Link zu der Freigabe mit der aktualisierten Version von cagsetup.exe, den MSI- und MST-Dateien angeben.

Konfigurieren von Single Sign-on für Windows-Betriebssysteme

Standardmäßig öffnen Windows-Benutzer eine Verbindung indem Sie das Secure Access Plug-in über das Startmenü aufrufen. Das Plug-in kann für Benutzer automatisch beim Anmelden an Windows gestartet werden, wenn Sie Single Sign-on aktivieren. Ist Single Sign-on konfiguriert, werden die Windows-Anmeldeinformationen des Benutzers zur Authentifizierung an das Access Gateway weitergegeben.

Aktivieren Sie Single Sign-on nur dann, wenn das Clientgerät sich an der Domäne Ihrer Organisation anmeldet. Wenn Single Sign-On aktiviert ist und Benutzer eine Verbindung von einem Clientgerät herstellen, das nicht in Ihrer Domäne ist, werden sie aufgefordert, sich anzumelden.

Wenn das Secure Access Plug-in für den Single Sign-On-Betrieb unter Windows konfiguriert ist, wird es automatisch gestartet, sobald sich Benutzer an Windows anmelden. Die Windows-Anmeldeinformationen des Benutzers werden zur Authentifizierung an das Access Gateway weitergegeben. Aktivieren von Single Sign-On für das Secure Access Plug-in ermöglicht Vorgänge auf dem Clientgerät wie Installationsskripte und die automatische Laufwerkszuordnung.

So konfigurieren Sie das Secure Access Plug-in für Windows-Single Sign-on

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Klicken Sie mit der rechten Maustaste im linken Bereich auf eine Gruppe und klicken Sie dann auf **Properties**.
3. Aktivieren Sie auf der Registerkarte **General** unter **Session options** die Option **Enable single sign-on with Windows** und klicken Sie auf **OK**.

Hinweis: Wenn Sie Zweimethodenauthentifizierung konfiguriert haben, ist die Verwendung von Single Sign-On nicht möglich.

Verbinden mit früheren Versionen des Access Gateway Plug-ins

Sie können das Access Gateway so konfigurieren, dass auch Verbindungen von früheren Versionen des Access Gateway Plug-ins akzeptiert werden. Beispielsweise können Sie Access Gateway Version 4.6 so konfigurieren, dass Verbindungen vom Access Gateway Plug-in Version 4.5 angenommen werden.

Wenn Sie Verbindungen mit früheren Versionen des Access Gateway Plug-ins zulassen möchten, stellen Sie den Verschlüsselungstyp für Clientverbindungen auf 3DES oder RC4 ein. Frühere Versionen des Access Gateway Plug-ins unterstützen keine AES-Verschlüsselung und können keine Verbindung aufbauen, wenn AES aktiviert ist.

So aktivieren Sie frühere Versionen des Access Gateway Plug-ins für Verbindungen mit dem Access Gateway

1. Klicken Sie auf die Registerkarte **Global Cluster Policies**.
2. Wählen Sie **Allow connections using earlier versions of Access Gateway Plug-in**.
3. Klicken Sie auf **Submit**.

Aktualisieren von früheren Versionen des Access Gateway Plug-ins

Sie steuern, wie das Upgrade des Access Gateway Plug-ins von einer früheren Version geschehen soll.

Sie können wählen, ob das Access Gateway Plug-in aktualisiert wird. Wenn die aktuelle Version des Plug-ins auf dem Clientgerät installiert werden soll, können Sie das Upgrade erzwingen oder Benutzer auffordern, das Upgrade zuzulassen. Wenn Benutzer das Upgrade nicht machen sollen, wählen Sie die Einstellung, die keine automatischen Upgrades zulässt.

Bei Access Gateway Plug-in-Versionen vor 4.5 ist diese Einstellung wirkungslos. Bei diesen Versionen werden Benutzer durch eine integrierte Funktion zum Upgrade aufgefordert, wenn sie versuchen, eine Verbindung zu einer höheren Version des Access Gateways herzustellen.

Wenn Benutzer das Plug-in aktualisieren sollen, werden Benutzer zum Upgrade aufgefordert, wenn beide der folgenden Bedingungen erfüllt sind:

- Das Access Gateway Plug-in von Access Gateway Version 4.5 wird zu einem späteren Zeitpunkt durch eine aktualisierte Version ersetzt
- Ein Benutzer stellt über Access Gateway Plug-in Version 4.5 eine Verbindung zum Access Gateway her.

So werden Upgrades von früheren Versionen des Access Gateway Plug-ins erzielt

1. Klicken Sie auf die Registerkarte **Global Cluster Policies**.
2. Tun Sie Folgendes:
   - Wählen Sie **Prompt to upgrade earlier versions of Access Gateway Plug-in**

   – Oder –

   - Wählen Sie **Force upgrade to earlier versions of the Access Gateway Plug-in**
3. Klicken Sie auf **Submit**.

Wenn Benutzer das Access Gateway Plug-in nicht aktualisieren sollen, wählen Sie **Do not upgrade earlier versions of the Access Gateway Plug-in**.

Herstellen einer Verbindung mit einer Webadresse

Wenn Benutzer eine Verbindung über eine Webseite herstellen, werden sie entweder aufgefordert, sich anzumelden, oder sie werden direkt an eine Portalseite weitergeleitet, auf der sie die Verbindung über das Access Gateway Plug-in herstellen können.

Ist das Access Gateway so konfiguriert, dass die Benutzer sich anmelden müssen, bevor sie eine Verbindung über das Access Gateway Plug-in herstellen können, geben sie dazu ihren Benutzernamen und ihr Kennwort ein. Eine Portalseite wird angezeigt, die die Anmeldung mit dem Access Gateway Plug-in oder mit dem Citrix XenApp Plug-in anbietet. Wenn Benutzer sich über das Access Gateway Plug-in anmelden, bietet die Verbindung uneingeschränkten Zugriff auf die Netzwerkressourcen, auf die die Gruppen, denen die Benutzer angehören, zugreifen dürfen.

Der durch die Sicherheitsrichtlinien gewährte Zugriff ermöglicht Benutzern, mit dem Remotesystem genau so zu arbeiten, als wären sie lokal angemeldet. Beispielsweise könnten Benutzer das Recht haben, auf Anwendungen zuzugreifen, einschließlich Web-, Client-Server- und Peer-to-Peer-Anwendungen wie Instant Messaging und Videokonferenzen. Die Benutzer können auch Netzlaufwerke zuordnen, um auf für sie zugängliche Netzwerkressourcen, wie z. B. freigegebene Ordner und Drucker, zuzugreifen.

Während der Verbindung mit dem Access Gateway können Remotebenutzer keine Netzwerkinformationen von der Site aus sehen, mit der sie verbunden sind. Geben Sie z. B. an einer Eingabeaufforderung Folgendes ein, während Sie mit dem Access Gateway verbunden sind:

ipconfig/all oder route print

Es werden keine Netzwerkinformationen aus dem gesicherten Netzwerk angezeigt.

Wenn Benutzer sich mit einem Webbrowser zum ersten Mal verbinden, installieren sie das Access Gateway Plug-in von der Portalseite. Wenn Benutzer auf der Portalseite auf **Citrix Access Gateway** klicken, geschieht Folgendes:

- Download und Installation des Plug-ins wird automatisch von der Webseite gestartet, statt die ausführbare Datei des Access Gateway Plug-in manuell herunterladen und installieren zu müssen.
- Wenn eine Vorauthentifizierungsrichtlinie auf dem Access Gateway konfiguriert ist, wird das Citrix Prescan Plug-in installiert und das Plug-in führ die Vorauthentifizierungsscans auf dem Clientgerät durch. Das Prescan Plug-in wird vor dem Access Gateway Plug-in installiert.
- Es bietet Single Sign-On-Funktionalität unter Windows für das Plug-in. Wenn das Access Gateway Plug-in über die Webseite gestartet wird, fordert das Plug-in die Benutzer nicht noch einmal auf, sich anzumelden.

Anmelden mit dem Access Gateway Plug-in

Wenn das Secure Access Plug-in geladen ist, werden die Benutzer aufgefordert, sich am Access Gateway anzumelden, damit die Verbindung hergestellt wird. Der Access Gateway-Administrator legt auf der Registerkarte **Authentication** im Administration Tool den Typ der Authentifizierung fest. Weitere Informationen hierzu finden Sie unter "Konfigurieren der Authentifizierung und Autorisierung" auf Seite 71.

Wenn auf dem Access Gateway Zweimethodenauthentifizierung konfiguriert ist und die Benutzer sich mit vollen Zugriffsberechtigungen anmelden, müssen sie für jedes Authentifizierungsverfahren den entsprechenden Benutzernamen und das zugehörige Kennwort eingeben. So könnte z. B. festgelegt werden, dass die Benutzer die LDAP-Authentifizierung und RSA SecurID verwenden müssen. In diesem Fall müssten die Benutzer ihr Kennwort, ihre RSA SecurID-PIN und den RSA SecurID-Code eingeben.

Hinweis: Wenn Sie das Citrix Access Gateway Plug-in für Linux verwenden, stehen die im Folgenden beschriebenen Optionen nicht im Verbindungsfenster zur Verfügung.

Das Access Gateway Plug-in wird installiert, sobald Benutzer sich das erste Mal an der Portalwebseite anmelden.

So installieren Sie das Access Gateway Plug-in

1. Geben Sie in einem Webbrowser die Webadresse des Access Gateways ein (z. B. *https://www.meinefirma.com*).
2. Wenn für das Access Gateway eine Anmeldung erforderlich ist, geben Sie den Benutzernamen und das Kennwort ein und klicken Sie auf **Anmelden**.
3. Auf der Portalseite des Citrix Access Gateways klicken Sie auf **Citrix Access Gateway** und folgen den Anweisungen auf dem Bildschirm, um das Access Gateway Plug-in zu installieren.

Nach der Installation müssen Benutzer sich noch einmal anmelden. Sie verwenden dazu das Symbol oder das Startmenü.

So melden Sie sich mit dem Access Gateway Plug-in am Access Gateway an

1. Klicken Sie auf **Start > Alle Programme > Citrix > Citrix Access Clients > Citrix Access Gateway**.
2. Geben Sie im Dialogfeld Citrix **Access Gateway** die Anmeldeinformationen ein.

   Wenn das Access Gateway mit mehreren Authentifizierungsbereichen konfiguriert ist und eine Verbindung zu einem anderen Bereich als dem Bereich *Default* hergestellt werden soll, geben Sie vor dem Benutzernamen den Bereichsnamen ein (*Bereichsname*\Benutzername).

   Falls SafeWord-Produkte von Secure Computing verwendet werden, geben Sie den Passcode ein.
3. Wenn das Access Gateway die Zweimethodenauthentifizierung erfordert, geben Sie für jedes Authentifizierungsverfahren den entsprechenden Benutzernamen und das zugehörige Kennwort ein.

   Wenn Ihre Site die RSA SecurID-Authentifizierung verwendet, setzt sich Ihr Kennwort aus Ihrer PIN und der auf dem RSA SecurID-Token angezeigten Zahl zusammen.

.

Das Access Gateway-Dialogfeld für die Zweimethodenauthentifizierung

4. Sollen die Einstellungen geändert werden, klicken Sie mit der rechten Maustaste auf das Dialogfeld und klicken Sie dann auf **Erweiterte Optionen**. Sie können die folgenden Einstellungen ändern:

   - **Webadresse** des Geräts: Hier werden außerdem die IP-Adressen oder vollqualifizierten Domänennamen der letzten 10 Geräte aufgeführt, zu denen Benutzer eine Verbindung hergestellt haben.
   - **Proxyeinstellungen** für das Clientgerät: Benutzer können automatische Proxyservererkennung festlegen oder einen Proxyserver manuell konfigurieren.
   - **Split DNS aktivieren**: Diese Einstellung wird im Administration Tool festgelegt. Ist diese Einstellung nicht verfügbar, sind entsprechend keine Änderungen möglich. Weitere Informationen über Split DNS finden Sie unter "Split DNS aktivieren" auf Seite 161.
   - **Sicherheitszertifikatswarnungen deaktivieren**: Falls kein von einer Zertifizierungsstelle signiertes sicheres Zertifikat installiert ist, wird eine Zertifikatswarnung eingeblendet, sobald sich ein Benutzer anmeldet. Diese Einstellung deaktiviert die Warnung.

Kontextmenü des Access Gateway-Dialogfelds

5. Sie können das zweite Kennwortfeld ein- und ausblenden. Führen Sie hierzu einen der folgenden Schritte aus:

   - Wird das Feld für das sekundäre Kennwort angezeigt, klicken Sie mit der rechten Maustaste auf eine beliebige Stelle im Dialogfeld und wählen Sie im Menü die Option **Sekundäres Kennwort ausblenden**.
   - Wird das Feld für das sekundäre Kennwort nicht angezeigt, klicken Sie mit der rechten Maustaste auf eine beliebige Stelle im Dialogfeld und wählen Sie im Menü die Option **Sekundäres Kennwort anzeigen**.

   Hinweis: Die Kennwortbeschriftungen im Dialogfeld **Citrix Access Gateway** können im Administration Tool auf der Registerkarte **Authentication** geändert werden. Falls Sie die Kennwortbeschriftungen geändert haben, wird dieser Text im **Citrix Access Gateway**-Dialogfeld und auf der Anmeldewebseite angezeigt. Die Menüoption zum Ein- und Ausblenden der Kennwortbeschriftungen bleibt unverändert. Weitere Informationen hierzu finden Sie unter "Ändern der Beschriftung von Kennwortfeldern" auf Seite 110.

6. Klicken Sie auf **Verbinden**.

Hinweis: Wenn das auf dem Access Gateway installierte digitale Zertifikat nicht von einer Zertifizierungsstelle signiert ist, wird eine Sicherheitswarnung angezeigt. Weitere Informationen finden Sie unter "Erstellen und Installieren von Zertifikaten" auf Seite 51 und "Sichern von Verbindungen mit digitalen Zertifikaten" auf Seite 223.

Wenn die Verbindung hergestellt ist, wird kurz ein Statusfenster angezeigt und das Secure Access **Plug-in**-Fenster wird auf ein Symbol im Infobereich der Taskleiste minimiert. Das Symbol zeigt, ob die Verbindung aktiviert oder deaktiviert ist und zeigt ggf. Statusmeldungen an.

So zeigen Sie die Access Gateway Plug-in-Statuseigenschaften an, wenn Benutzer angemeldet sind

Doppelklicken Sie im Infobereich auf das Access Gateway-Verbindungssymbol. Sie können stattdessen auch mit der rechten Maustaste auf das Symbol klicken und im Kontextmenü den Befehl **Eigenschaften** wählen.

Das **Citrix Access Gateway**-Dialogfeld wird angezeigt.

Die Verbindungseigenschaften enthalten nützliche Informationen für die Problembehandlung. Hierzu gehören z. B. folgende Eigenschaften:

- Die Registerkarte **Allgemein** enthält Verbindungsinformationen.
- Auf der Registerkarte **Details** finden Sie Serverinformationen und eine Liste der gesicherten Netzwerke, auf die der Client zugreifen kann.
- Die Registerkarte **Zugriffslisten** enthält die Zugriffssteuerungslisten (ACLs), die für die Benutzerverbindung konfiguriert sind. Diese Registerkarte wird nur für Benutzer angezeigt, die Mitglied einer Gruppe sind. Wenn für eine Gruppe keine Zugriffssteuerungsliste konfiguriert ist, wird die Registerkarte auch nicht angezeigt.

Klicken Sie zum Schließen des Fensters auf **Schließen**.

So trennen Sie das Access Gateway Plug-in

Klicken Sie mit der rechten Maustaste im Infobereich der Taskleiste auf das Secure Access-Symbol und wählen Sie im Kontextmenü den Befehl **Trennen**.

Installieren des Access Gateway Plug-ins für Linux

Das Access Gateway Plug-in unterstützt Linux Kernel 2.6.

Wenn Benutzer sich mit dem Access Gateway Plug-in für Linux anmelden, empfiehlt Citrix das Plug-in für externe Verbindungen zu verwenden (z. B. über das Internet) und nicht für Verbindungen vom internen Netzwerk.

Wenn die Verbindung von einem Linux-Computer hergestellt wird, klicken Sie auf **Download**, um den Download zu starten und die Anweisungen für die Installation des Access Gateway Plug-in für Linux anzuzeigen.

Wichtig: Damit das Access Gateway Plug-in für Linux korrekt funktioniert, aktivieren Sie Split-Tunneling auf dem Access Gateway.

Bevor Sie das Access Gateway Plug-in für Linux installieren, sollte der Linux TUN/TAP-Treiber auf dem Clientgerät installiert sein. Wenn er nicht installiert ist, wählen Sie in der Kernelkonfiguration **Device Drivers > Network device support > Universal TUN/TAP device drive support**. Nachdem dies ausgewählt ist, kompilieren Sie den Kernel neu.

Außerdem muss auch das Stat-Dienstprogramm auf dem Clientgerät installiert sein. Sie können das Stat-Dienstprogramm mit dem Coreutils-Paket des Linux-Systems installieren.

Außer dem Befehl **cagvpn --login**, mit dem Sie den Anmeldevorgang für das Access Gateway Plug-in für Linux starten, können Sie mit **cagvpn --help** eine Liste der anderen Befehlzeilenoptionen anzeigen. Wenn die Verbindung getrennt wird, wird der VPN-Dämon u. U. gestoppt.

Für das Secure Access Plug-in für Linux ist ein VPN-Daemon für die Verbindung mit dem Access Gateway erforderlich. Wenn Sie den Status des VPN-Dämons prüfen möchten, geben Sie an einer Eingabeaufforderung Folgendes ein:

/etc/init.d/cagvpnd status

Wenn der Daemon nicht ausgeführt wird, geben Sie Folgendes ein:

/etc/init.d/cagvpnd start

Zum Neustarten eines gestoppten Dämons geben Sie Folgendes ein:

/etc/init.d/cagvpnd start

So entfernen Sie das Access Gateway Plug-in für Linux

1. Geben Sie an einer Eingabeaufforderung Folgendes ein:

   cagvpn_uninstall

Hiermit werden alle Binärdateien sowie andere Datei des Access Gateway Plug-ins für Linux entfernt. Weitere Informationen finden Sie in der Datei CitrixVPN_ReadMe.txt im Stammverzeichnis.

Wenn auf dem Clientgerät eine Firewall ausgeführt wird, müssen Benutzer sie eventuell deaktivieren oder die Einstellungen ändern. Firewallregeln beeinträchtigen möglicherweise den Paketbehandlungsmechanismus des Access Gateway Plug-ins für Linux. Weitere Informationen finden Sie in der Dokumentation des Firewallherstellers.

Hinweis: Das ICMP-Protokoll wird derzeit nicht vom Access Gateway Plug-in für Linux unterstützt.

Konfigurieren der Authentizierungsanforderungen nach einer Netzwerkunterbrechung

Wenn die Netzwerkverbindung kurz unterbrochen wird, müssen sich Benutzer standardmäßig nicht neu anmelden, sobald die Verbindung wiederhergestellt ist. Sie können allerdings vorschreiben, dass Benutzer sich nach einer Unterbrechung doch neu anmelden müssen, z. B. wenn sich ein Computer im Ruhezustand oder Standby-Modus befunden hat, wenn Benutzer in ein anderes drahtloses Netzwerk wechseln oder wenn eine Verbindung erzwungenermaßen beendet wurde.

Hinweis: Das Access Gateway versucht, Benutzer mit dem gecachten Kennwort zu authentifizieren. Wenn Benutzer sich mit einem Einmal-Kennwort anmelden, wie etwa von einem RSA SecurID-Token, schlägt die Authentifizierung am Access Gateway fehl und die Benutzer können sich nicht anmelden oder werden gar gesperrt. Damit diese Einmal-Kennwörter nicht wieder verwendet werden, können Sie das Access Gateway so konfigurieren, dass Benutzer sich nach einer Netzwerkunterbrechung neu anmelden müssen. Weitere Informationen hierzu finden Sie unter "Konfigurieren der Authentifizierung für die Verwendung von Einmal-Kennwörtern" auf Seite 107.

So erzwingen Sie die Neuanmeldung von Benutzern nach einer Netzwerkunterbrechung oder einem Ruhezustand

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Klicken Sie mit der rechten Maustaste im linken Bereich auf eine Gruppe und klicken Sie dann auf **Properties**.
3. Aktivieren Sie auf der Registerkarte **General** unter **Session options** eine oder beide der folgenden Optionen:
   - **Authenticate after network interruption:** Mit dieser Option müssen sich Benutzer neu anmelden, wenn die Netzwerkverbindung kurz unterbrochen war.
   - **Authenticate upon system resume:** Mit dieser Option müssen sich Benutzer neu anmelden, wenn sich die Computer im Standby-Modus oder Ruhezustand waren. Diese Option bietet ein höheres Maß an Sicherheit für unbeaufsichtigte Computer.
4. Klicken Sie auf **OK**.

Hinweis: Wenn Sie eine Verbindung schließen und einen Benutzer oder eine Gruppe daran hindern möchten, automatisch wieder eine Verbindung herzustellen, müssen Sie die Einstellung **Authenticate after network interruption** aktivieren. Anderenfalls stellen die Benutzer unverzüglich eine neue Verbindung her, ohne dabei nach ihren Anmeldeinformationen gefragt zu werden.

Konfigurieren weiterer Gruppeneigenschaften

Mit zusätzlichen Gruppenrichtlinien können Sie den Zugriff der Benutzer auf das Netzwerk weiter konfigurieren:

- "Aktivieren von IP-Pooling"
- "Split DNS aktivieren"
- "Aktivieren von internem Failover"
- "Aktivieren von Domänenanmeldeskripten"
- "Aktivieren von Sitzungstimeouts für Access Gateway Plug-ins"
- "Konfigurieren von Websitzungstimeouts"

Aktivieren von IP-Pooling

In manchen Situationen brauchen Benutzer, die sich mit dem Secure Access Plug-in verbinden, eine einzigartige IP-Adresse für das Access Gateway. So muss z. B. in einer Samba-Umgebung jeder Benutzer, der eine Verbindung zu einem zugewiesenen Netzlaufwerk herstellt, den Eindruck erwecken, dass er sich von einer anderen IP-Adresse aus anmeldet. Wenn Sie das IP-Pooling für eine Gruppe aktivieren, kann das Access Gateway jedem Client einen eindeutigen IP-Adressalias zuweisen.

Sie können das Gatewaygerät angeben, das für das IP-Pooling verwendet werden soll. Als Gatewaygerät kommen sowohl das Access Gateway selbst als auch einige andere Geräte infrage. Wenn Sie kein Gateway festlegen, wird auf der Basis der Einstellungen auf der Registerkarte "General Networking" eine Access Gateway-Schnittstelle verwendet, wobei Folgendes gilt:

- Wenn Sie nur die Schnittstelle 0 konfiguriert haben (das Access Gateway ist innerhalb der Firewall), wird die IP-Adresse der Schnittstelle 0 als Gateway verwendet.
- Wenn Sie die Schnittstellen 0 und 1 konfiguriert haben (das Access Gateway ist in der DMZ), wird die IP-Adresse der Schnittstelle 1 als Gateway verwendet. In diesem Szenario ist Schnittstelle 1 die interne Schnittstelle.

Die IP-Poolingkonfiguration muss auf allen gleichartigen Access Gateway-Geräten im Cluster konsistent sein. Wenn es in dem Cluster Gerät1, Gerät2 und Gerät3 gibt, konfigurieren Sie das IP-Pooling auf dem Gerät, das die Einstellungen veröffentlicht. Wenn die Einstellungen veröffentlicht wurden, werden die IP-Pooling-Informationen auf die anderen Geräte in dem Cluster repliziert.

Wenn Sie einem Cluster, in dem das IP-Pooling konfiguriert ist, ein Access Gateway hinzufügen, werden die IP-Poolinginformationen entfernt. Wenn Sie das IP-Pooling auf dem neuen Gerät konfigurieren nach Sie es dem Cluster hinzugefügt haben, erhalten Benutzer nicht die Adressen aus dem Pool.

So konfigurieren Sie IP-Pooling für eine Gruppe

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Klicken Sie mit der rechten Maustaste im linken Bereich auf eine Benutzergruppe und klicken Sie dann auf **Properties**.
3. Aktivieren Sie auf der Registerkarte **Network** die Option **Enable IP pools**.
4. Klicken Sie mit der rechten Maustaste unter **IP pool configuration** auf ein Gateway und klicken Sie dann auf **Change the IP Address Pool**.
5. Geben Sie unter **Starting IP Address** die erste IP-Adresse des Pools ein.
6. Geben Sie unter **Number of IP addresses** die Anzahl der IP-Adressaliasse ein. In allen IP-Pools können insgesamt bis zu 2000 IP-Adressen vorhanden sein.

7. Geben Sie unter **Default gateway** die IP-Adresse des Gateways ein.

   Wenn Sie dieses Feld leer lassen, wird ein Access Gateway-Netzwerkadapter verwendet, wie dies bereits weiter oben in diesem Abschnitt beschrieben wurde. Wenn Sie ein anderes Gerät als Gateway festlegen, fügt das Access Gateway der Access Gateway-Routingtabelle einen Eintrag für diese Route hinzu.

8. Klicken Sie zweimal auf **OK**.

Split DNS aktivieren

Standardmäßig überprüft das Access Gateway lediglich das Remote-DNS des Benutzers. Durch Aktivieren von Split DNS können Sie Failoveroperationen auf das lokale DNS des Benutzers zulassen. Diese Einstellung kann im Dialogfeld **Verbindungseigenschaften** im Dialogfeld **Access Gateway** außer Kraft gesetzt werden.

So aktivieren Sie Split DNS

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Klicken Sie mit der rechten Maustaste im linken Bereich auf eine Gruppe und klicken Sie dann auf **Properties**.
3. Klicken Sie auf der Registerkarte **Network** auf **Enable split DNS** und klicken Sie dann auf **OK**.

   Das Access Gateway führt lediglich dann eine Failoveroperation auf das lokale DNS durch, wenn kein Kontakt zu den angegebenen DNS-Servern hergestellt werden kann. Bei erfolgreicher Kontaktaufnahme, aber negativer Antwort erfolgt kein Failover.

Aktivieren von internem Failover

Durch Konfigurieren der lokalen DNS-Einstellungen des Clients, kann das Access Gateway Plug-in die Verbindung zum Access Gateway von innerhalb der Firewall herstellen. Wenn diese Einstellungen konfiguriert sind, führt der Client ein Failover zur internen IP-Adresse des Access Gateways durch, falls die externe IP-Adresse nicht erreichbar ist.

So aktivieren Sie das interne Failover

1. Klicken Sie auf die Registerkarte **Global Cluster Policies**.
2. Aktivieren Sie unter **Advanced options** die Option **Enable internal failover**.

Wenn dieses Kontrollkästchen aktiviert ist, wird die interne IP-Adresse des Access Gateway in die Failoverliste aufgenommen. Falls Sie externen Administratorzugriff deaktiviert haben, steht Port 9001 nicht zur Verfügung. Soll eine Verbindung zu Port 9001 hergestellt werden, wenn Sie sich über eine externe Verbindung anmelden, konfigurieren Sie die IP-Pools und stellen Sie die Verbindung zur niedrigsten IP-Adresse im IP-Pool her.

Aktivieren von Domänenanmeldeskripten

Im Netzwerk sind ggf. Anmeldeskripte vorhanden, die nach einer erfolgreichen Anmeldung auf dem Clientgerät ausgeführt werden. Wenn auf dem Access Gateway Anmeldeskripte aktiviert sind, richtet das Access Gateway nach der Authentifizierung die Verbindung ein, ruft die Windows-Anmeldeskripte vom Domänencontroller ab und führt diese aus, um Operationen wie die automatische Laufwerkszuordnung auszuführen.

Hinweis: Voraussetzung dafür, dass Benutzer die Single Sign-On-Funktion unter Windows XP sowie die Anmeldeskripte verwenden können, ist die Anmeldung als Hauptbenutzer oder die Mitgliedschaft in der Gruppe der Hauptbenutzer.

Das Access Gateway kann Anmeldeskripte ausführen, die im Windows-Profil des Benutzers definiert sind. Anmeldeskripts, die in Active Directory definiert sind, werden nicht unterstützt und folglich auch nicht ausgeführt.

Wenn kein Kontakt zum Domänencontroller hergestellt werden kann, wird zwar die Access Gateway-Verbindung hergestellt, die Anmeldeskripte werden aber nicht ausgeführt.

Wichtig: Das Clientgerät muss ein Mitglied der Domäne sein, damit Domänenanmeldeskripte ausgeführt werden können.

So aktivieren Sie Anmeldeskripte

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Klicken Sie mit der rechten Maustaste im linken Bereich auf eine Gruppe und klicken Sie dann auf **Properties**.
3. Aktivieren Sie auf der Registerkarte **General** unter **Session options** die Option **Run logon scripts**. Klicken Sie auf **OK**.

Hinweis: Die Anmeldeskriptunterstützung ist beschränkt auf Skripte, die von der Befehlsverarbeitung ausgeführt werden, wie z. B. EXE- und BAT-Dateien. Visual Basic- und JavaScript-Anmeldeskripte werden nicht unterstützt.

Aktivieren von Sitzungstimeouts für Access Gateway Plug-ins

Sie können das Access Gateway Plug-in so konfigurieren, dass die Trennung der Verbindung zum Access Gateway erzwungen wird, falls während eines bestimmten Zeitraums (in Minuten) keinerlei Aktivitäten über die Verbindung zu verzeichnen sind. Eine Minute vor dem Timeout (also der Trennung) der Sitzung erhalten Benutzer eine Warnmeldung, dass die Sitzung in Kürze geschlossen wird. Falls die Sitzung tatsächlich geschlossen wird, müssen Benutzer sich neu anmelden.

Beim Konfigurieren eines Werts für ein Sitzungstimeout stehen drei Optionen zur Auswahl:

- **User session time-out: (Benutzersitzungstimeout)** Mit dieser Einstellung trennt das Access Gateway Plug-in die Verbindung nach Ablauf der Timeoutfrist, unabhängig von den aktuellen Aktivitäten des Benutzers. Benutzer haben keine Möglichkeit, diese Trennung nach Ablauf der Timeoutfrist zu vermeiden.
- **Network inactivity time-out**: (Netzwerkinaktivitätstimeout) Mit dieser Einstellung trennt das Access Gateway Plug-in die Verbindung, wenn während des angegebenen Zeitraums keine Netzwerkpakete mehr vom Clientgerät an das Access Gateway gesendet werden.
- **Idle session time-out**: (Timeout wegen inaktiver Sitzung) Mit dieser Einstellung wird die Benutzersitzung beendet, wenn während des angegebenen Zeitraums die Maus oder die Tastatur nicht mehr benutzt werden.

Zum Aktivieren dieser Einstellungen geben Sie jeweils den Zeitraum in Minuten für die Timeoutfrist ein (zulässige Werte: 1 bis 65536). Mit dem Wert Null (0) deaktivieren Sie die jeweilige Einstellung. Wenn Sie den Wert "0" eingeben, wird das Sitzungstimeout nicht aktiviert und die Einstellung wirkt sich nicht auf Clientverbindungen aus.

Falls Sie mehrere Einstellungen gleichzeitig aktivieren, wird die Clientverbindung geschlossen, sobald die erste Timeoutfrist abläuft.

So aktivieren Sie Sitzungstimeouts

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Klicken Sie mit der rechten Maustaste im linken Bereich auf eine Gruppe und klicken Sie dann auf **Properties**.
3. Geben Sie auf der Registerkarte **General** unter **Session options** den Zeitraum in Minuten für die folgenden Einstellungen ein:
   - User session time-out (Benutzersitzungstimeout)
   - Network inactivity time-out (Netzwerkinaktivitätstimeout)
   - Idle session time-out (Timeout wegen inaktiver Sitzung)
4. Klicken Sie auf **OK**.

Konfigurieren von Websitzungstimeouts

Wenn Benutzer sich mit der Anmeldeseite am Access Gateway anmelden, werden Cookies gesetzt, um zu ermitteln, ob die Websitzung noch auf dem Access Gateway aktiv ist. Wenn das Access Gateway-Cookie abläuft und die Authentifizierung über die Anmeldeseite aktiviert ist, werden Benutzer aufgefordert, die Authentifizierungsinformationen einzugeben, damit er die Websitzung wieder aufnehmen kann. Damit wird der Zeitraum beschränkt, in dem Netzwerkangriffe über eine unbeaufsichtigte Websitzung erfolgen könnten, sodass ein gewisser Grad an Sicherheit entsteht.

So aktivieren Sie das Websitzungstimeout

1. Klicken Sie auf die Registerkarte **Global Cluster Policies**.
2. Geben Sie unter **Access options** den Zeitraum in Minuten in das Feld **Web session time-out** ein.

   Soll das Websitzungstimeout deaktiviert werden, geben Sie den Wert **0** in das Textfeld ein.

Anfordern von Clientzertifikaten für die Authentifizierung

Wenn Sie auf eine zusätzliche Authentifizierung Wert legen, können Sie das Access Gateway so konfigurieren, dass Clientzertifikate zur Authentifizierung angefordert werden.

Das Access Gateway kann Clientzertifikate in den folgenden Speicherorten authentifizieren:

- Im Zertifikatspeicher des Windows-Betriebssystems auf einem Clientgerät. In diesem Fall wird das Zertifikat unter Verwendung der Microsoft Management Console (MMC) separat im Zertifikatspeicher installiert.
- Auf einer Smartcard oder einem Hardwaretoken. In diesem Fall ist das Zertifikat in die Smartcard eingebettet und wird über einen Smartcardleser eingelesen, der mit dem Netzwerk verbunden ist.

Hinweis: Die Konfiguration des Access Gateways bleibt gleich, unabhängig davon, ob die Zertifikate im Windows-Betriebssystem oder auf einer Smartcard gespeichert sind. Zur Unterstützung von Clientzertifikaten an diesen Speicherorten ist keine besondere Konfiguration erforderlich.

Wenn Sie das Access Gateway so konfigurieren, dass Clientzertifikate angefordert werden, müssen alle Benutzer, die sich über das Access Gateway anmelden, ein sicheres Clientzertifikat vorlegen. Das Zertifikat kann daher aus dem Zertifikatspeicher in Windows oder von einer Smartcard stammen.

So legen Sie fest, dass Clientzertifikate erforderlich sein sollen

1. Klicken Sie auf die Registerkarte **Global Cluster Policies**.
2. Wählen Sie unter **Select security options**, die Option **Require secure client certificates** und klicken Sie auf **Submit**.

Definieren von Clientzertifikatskriterien

Verwenden Sie zum Festlegen der Kriterien, die die Clientzertifikate erfüllen müssen, einen booleschen Ausdruck. Damit Benutzer einer Gruppe angehören können, müssen sie nicht nur alle anderen für die jeweilige Gruppe konfigurierten Authentifizierungsregeln einhalten, sondern auch die Zertifikatskriterien erfüllen. So erfordern z. B. die folgenden Kriterien, dass im Betreff-Feld des vom jeweiligen Benutzer bereitgestellten Clientzertifikats für die Organisationseinheit (Organizational Unit, OU) Buchhaltung und für den gemeinsamen Namen (Common Name, CN) ein Wert festgelegt ist, der mit dem lokalen Benutzernamen des Benutzers auf dem Access Gateway übereinstimmt.

client_cert_end_user_subject_organizational_unit="Buchhaltung" und username=client_cert_end_user_subject_common_name.

Folgende Operatoren können verwendet werden:

and, logisches UND

= Übereinstimmungsprüfung

Gültige Konstanten für die Kriterien:

*true***,** logisches WAHR

Gültige Variablen für die Kriterien:

username lokaler Benutzername auf dem Access Gateway*client_cert_end_user_subject_common_name* CN-Attribut des Betreffs des Clientzertifikats *client_cert_end_user_subject_organizational_unit* OU-Attribut des Betreffs des Clientzertifikats certificate*client_cert_end_user_subject_organization* O-Attribut des Betreffs des Clientzertifikats

Die Werte für die Clientzertifikatskriterien müssen in Anführungszeichen gesetzt werden. Beispiele für richtige und falsche Schreibweise:

Der boolesche Ausdruck *client_cert_end_user_subject_common_name="clients.gateways.citrix.com"* ist gültig und funktioniert.

Der boolesche Ausdruck *client_cert_end_user_subject_common_name=clients.gateways.citrix.com* ist ungültig und funktioniert nicht.

So legen Sie die Clientzertifikatskonfiguration fest

1. Klicken Sie mit der rechten Maustaste auf der Registerkarte **Access Policy Manager** auf eine andere Gruppe als die Standardgruppe und klicken Sie dann auf **Properties**.

   Hinweis: Für die Standardbenutzergruppe ist die Clientzertifikatskonfiguration nicht verfügbar.

2. Geben Sie auf der Registerkarte **Client Certificate** unter **Client certificate criteria expression** die Zertifikatsinformationen ein und klicken Sie auf **OK**.

Verwenden von Clientzertifikaten mit Access Gateway Advanced Edition

Sowohl für das Access Gateway als auch für die Server, auf denen Advanced Edition ausgeführt wird, kann die Verwendung sicherer Clientzertifikate angefordert werden. Beachten Sie die folgenden Hinweise beim Konfigurieren der Verwendung von Clientzertifikaten:

- Das Access Gateway Plug-in kann Zertifikate aus dem Windows-Benutzerprofil, von einer Smartcard oder einem Hardwaretoken lesen, das die Microsoft Crypto-API unterstützt.
- Das Clientzertifikat stellt keine Authentifizierung des Benutzers dar, sondern fungiert lediglich als zusätzliche Clientbedingung, z. B. ein Endpunktscan. Die Benutzer müssen nach wie vor ihr Kennwort oder ihren Tokencode eingeben.

Installieren von Stammzertifikaten

Auf allen Clientgeräten, die über das Access Gateway eine Verbindung zum sicheren Netzwerk herstellen, muss ein Stammzertifikat vorliegen.

Das Windows-Betriebssystem und Internet Explorer unterstützen bereits die meisten vertrauenswürdigen Stammzertifizierungsstellen. Bei diesen Zertifizierungsstellen ist es also nicht nötig, Stammzertifikate abzurufen und auf dem Clientgerät zu installieren. Wenn Sie jedoch eine andere Zertifizierungsstelle verwenden, müssen Sie die entsprechenden Stammzertifikate selbst abrufen und installieren.

Abrufen eines Stammzertifikats von einer Zertifizierungsstelle

Stammzertifikate sind bei denselben Zertifizierungsstellen erhältlich wie Serverzertifikate. Bekannte und vertrauenswürdige Zertifizierungsstellen sind beispielsweise Verisign, Baltimore, Entrust und die jeweils angeschlossenen Unternehmen.

Bei den Zertifizierungsstellen wird in der Regel vorausgesetzt, dass Sie bereits über geeignete Stammzertifikate verfügen. (Die meisten Webbrowser enthalten Stammzertifikate.) Wenn Sie jedoch Zertifikate von einer Zertifizierungsstelle heranziehen, die auf dem Clientgerät noch nicht genutzt wird, müssen Sie das Stammzertifikat explizit anfordern.

Es stehen mehrere Arten von Stammzertifikaten zur Auswahl. VeriSign bietet beispielsweise rund 12Stammzertifikate für verschiedene Zwecke an. Achten Sie also darauf, das jeweils richtige Stammzertifikat bei der Zertifizierungsstelle abzurufen.

Installieren von Stammzertifikaten auf einem Clientgerät

Stammzertifikate werden mit der Microsoft Management Console (MMC) unter Windows installiert. Hierbei kommt der Zertifikatsimport-Assistent zum Einsatz. Das Zertifikat wird unter den vertrauenswürdigen Stammzertifizierungsstellen für den lokalen Computer gespeichert.

Weitere Informationen zur Verfügbarkeit von Stammzertifikaten und zu deren Installation auf anderen Plattformen außer 32-Bit-Windows finden Sie in der Produktdokumentation für das jeweils verwendete Betriebssystem.

Auswählen einer Verschlüsselungsart für Clientverbindungen

Alle Kommunikation zwischen dem Access Gateway Plug-in und dem Access Gateway werden mit SSL verschlüsselt. Mit dem SSL-Protokoll sind zwei Computer in der Lage, Verschlüsselungssammlungen für die symmetrische Verschlüsselung von Daten über eine sichere Verbindung auszuhandeln.

Sie können die Verschlüsselungssammlung festlegen, die das Access Gateway für die symmetrische Datenverschlüsselung bei einer SSL-Verbindung verwendet. Die Auswahl einer starken Verschlüsselungssammlung senkt die Gefahr böswilliger Angriffe. Je nach den Sicherheitsrichtlinien Ihres Unternehmens müssen Sie außerdem ggf. eine bestimmte Verschlüsselungssammlung für die symmetrische Verschlüsselung über sichere Verbindungen festlegen.

Hinweis: Wenn Sie über das Access Gateway Zugriff auf Citrix XenApp bereitstellen, wird auch der ICA-Datenverkehr an das Access Gateway mit diesen Verschlüsselungssammlungen verschlüsselt.

Für SSL-Verbindungen stehen RC4-, 3DES- und AES-Verschlüsselungssammlungen zur Auswahl. Die Standardeinstellung ist RC4 128-Bit. Der MD5- oder SHA-Hash-Algorithmus wird zwischen dem Client und dem Server ausgehandelt.

Bei der Verschlüsselung sicherer Verbindungen mit öffentlichem Schlüssel wird RSA verwendet. Für die symmetrische Verschlüsselung stehen dabei die folgenden Verschlüsselungssammlungen und Hash-Algorithmen bereit:

- RC4 128-Bit, MD5/SHA
- 3DES, SHA
- AES 128/256-Bit, SHA

So wählen Sie eine Verschlüsselungsart für Clientverbindungen aus

1. Klicken Sie auf die Registerkarte **Global Cluster Policies**.
2. Wählen Sie unter **Select security options** im Feld **Select encryption type for client connections** die gewünschte Verschlüsselungssammlung für sichere Verbindungen aus und klicken Sie auf **Submit**.

Konfigurieren von Anmelde- und Portalseiten für das Citrix Access Gateway Plug-in

Das Access Gateway kann so konfiguriert werden, dass Benutzer die Anmeldeseite und die Portalseite verwenden. Auf der Anmeldeseite müssen Benutzer erst ihre Anmeldeinformationen eingeben und werden dann mit der Portalseite verbunden, auf der sich Benutzer mit dem Access Gateway Plug-in oder dem Webinterface anmelden können.

Dieses Kapitel enthält:

- "Konfigurieren der Access Gateway-Anmeldeseiten"
- "Access Gateway-Portalseitenvorlagen"
- "Konfigurieren einer Portalseite mit mehreren Anmeldeoptionen"
- "Anmelden, wenn Vorauthentifizierungsrichtlinien konfiguriert sind"

Konfigurieren der Access Gateway-Anmeldeseiten

Benutzer müssen sich an der Access Gateway-Anmeldeseite anmelden, bevor sie sich mit dem Access Gateway Plug-in oder über das Webinterface verbinden können. Sie haben die Wahl zwischen der Standardanmeldeseite, die Teil des Access Gateways ist, oder Sie können die Anmeldeseite mit Ihrem Firmenlogo, einem Cascading Stylesheet und Ihrem eigenen HTML-Fußzeilentext anpassen.

Aktivieren der Anmeldeseitenauthentifizierung

Standardmäßig müssen Benutzer sich an der Anmeldeseite anmelden und noch einmal am Secure Access Plug-in oder am Webinterface. Mit den folgenden beiden Methoden erreichen Sie, dass die Anmeldung an der Anmeldeseite entfällt:

- Sie können eine globale Richtlinie einrichten, mit der die Authentifizierung für die Anmeldeseite deaktiviert wird und die angibt, welche Anmeldeseite für alle Benutzer angezeigt wird. Diese globale Richtlinie setzt alle Anmeldeseitenfestlegungen für Gruppen außer Kraft.

So aktivieren Sie die Anmeldeseitenauthentifizierung

1. Klicken Sie auf die Registerkarte **Global Cluster Policies**.
2. Wählen Sie unter **Advanced options** die Option **Enable logon page authentication** und klicken Sie auf **Submit**.

Wenn das Kontrollkästchen **Enable logon page authentication** nicht aktiviert ist, melden sich Benutzer nicht an, sondern werden direkt zur benutzerdefinierten Portalseite weitergeleitet.

Anpassen der Anmeldeseite

Sie passen die Anmeldeseite an, indem Sie eigene Bilder hochladen, Stylesheets und Text verwenden. Nach dem Upload wird den Benutzern die angepasste Anmeldeseite anstelle der Standardseite angezeigt.

So passen Sie die Anmeldeseite auf dem Access Gateway an

1. Klicken Sie auf die Registerkarte **Portal Page Configuration**.
2. Wählen Sie auf der Registerkarte **Logon Page** in der Dropdownliste **Logon page type** die Option **Customized Logon Page** aus.

3. Wenn Sie eine angepasste Portalseite installieren, führen Sie die entsprechenden unten beschriebenen Tasks aus:

   - Um ein Bild hochzuladen, klicken Sie unter **Primary logo image** auf **Upload New Primary image**, wählen Sie die Bilddatei aus und klicken Sie dann auf **Öffnen**.

     Hinweis: Die Datei für die primäre Grafik sollte 14 KB groß und 300 Pixel breit mal 62 Pixel hoch sein. Wenn die Grafikdateigröße zwischen 14 und 50 KB ist, wird teilweise eine grüne Hintergrundfarbe im Administration Tool angezeigt und auf der Anmeldeseite wird das ganze Bild mit Bildlaufleisten dargestellt. Wenn die Grafikdatei größer als 50 KB ist, wird ein grauer Kasten im Administration Tool und auf der Anmeldeseite das ganze Bild angezeigt.

   - Um eine weitere Bilddatei hochzuladen, klicken Sie unter **Secondary logo image** auf **Upload New Secondary Image**.

     Hinweis: Für die Datei der sekundären Grafik gelten keine Dimensionsbeschränkungen und sie wird immer ohne Bildlaufleiste auf der Anmeldeseite angezeigt. Wenn die Grafikdateigröße zwischen 14 und 50 KB ist, wird teilweise eine grüne Hintergrundfarbe im Administration Tool angezeigt, aber auf der Anmeldeseite erscheint das ganze Bild. Wenn die Grafikdatei größer als 50 KB ist, wird ein grauer Kasten im Administration Tool und auf der Anmeldeseite das ganze Bild angezeigt.

   - Wenn Sie ein Stylesheet verwenden, können Sie unter **Style sheet** entweder das aktuelle Stylesheet herunterladen oder ein neues Stylesheet hochladen.
   - Um eine Fußzeile zu erstellen, geben Sie im Bereich **HTML footer** den Text ein und zum Schluss klicken Sie dann im oberen Bereich der Seite auf **Apply**.

Wählen Sie nach der Installation der angepassten Portalseite die Portalseite für die Benutzer aus. Weitere Informationen finden Sie an folgenden Stellen:

- Informationen zur Verwendung der Portalseite, die Teil des Geräts ist, finden Sie unter "Access Gateway-Portalseitenvorlagen" auf Seite 174.
- Informationen, wie Sie Benutzern die Wahl geben, sich entweder mit dem Access Gateway Plug-in oder mit dem Webinterface anzumelden, finden Sie unter "Konfigurieren einer Portalseite mit mehreren Anmeldeoptionen" auf Seite 178
- Informationen darüber, ob eine Vorauthentifizierungsrichtlinie konfiguriert ist, finden Sie unter "Anmelden, wenn Vorauthentifizierungsrichtlinien konfiguriert sind" auf Seite 179.

Access Gateway-Portalseitenvorlagen

Wenn Benutzer das Access Gateway Plug-in über einen Webbrowser starten, wird die Anmeldeseite des Citrix Access Gateways angezeigt. Nachdem sich Benutzer angemeldet haben, werden Sie an eine Portalseite weitergeleitet, auf der sie die Wahl haben, sich mit dem Access Gateway Plug-in oder über das Webinterface anzumelden.

Citrix stellt Portalseitenvorlagen zur Verfügung, die individuell angepasst werden können. Eine einfache Form der Anpassung der Standardportalseite ist das Ersetzen des Logos.

Der Text für **Citrix Access Gateway** verwendet eine Variable, die in den Text der Vorlage eingesetzt wird. Der Text kann nicht geändert werden.

Hinweis: Wenn Sie der Vorlage Text hinzufügen oder Formatänderungen vornehmen möchten, sollten Sie jemanden zurate ziehen, der sich mit HTML auskennt. Es werden nur die Änderungen an den Vorlagen unterstützt, die hier beschrieben werden.

Herunterladen von und Arbeiten mit Portalseitenvorlagen

Die Portalseitenvorlagen stehen im Administration Portal auf der Seite Downloads zur Verfügung.

Die Portalseitenvorlagen enthalten Variablen, die das Access Gateway durch den Namen des aktuellen Benutzers ersetzt und durch einen Link, mit dem das Access Gateway Plug-in gestartet wird.

Die für Vorlagen zur Verfügung stehenden Variablen werden in der folgenden Tabelle erklärt.

Variable	Durch Variable eingefügter Inhalt
$citrix_username;	Name des angemeldeten Benutzers
$citrix_portal_full_client_only;	Ausschließlich Link zum Secure Access Plug-in

So laden Sie die Portalseitenvorlagen auf den lokalen Computer herunter

1. Klicken Sie im Administration Portal auf **Downloads**.
2. Klicken Sie unter **Download a sample portal page template that includes** mit der rechten Maustaste auf **A link for the Access Gateway Plug-in**, klicken Sie auf **Save Target as** und geben Sie in dem Dialogfeld einen Speicherort an.

So passen Sie die Vorlage an

1. Überlegen Sie sich, wie viele benutzerdefinierte Portalseiten Sie benötigen. Portalseiten können für mehrere Gruppen verwendet werden.
2. Erstellen Sie Kopien der Vorlagen, die Sie verwenden möchten, und geben Sie ihnen einen Namen mit der Dateierweiterung .html.
3. Öffnen Sie die Datei im Windows-Editor oder einem HTML-Editor.
4. So ersetzen Sie das Citrix Logo
   A. Gehen Sie in der Vorlage zu der folgenden Zeile:
   B. Setzen Sie für **citrix-logo.gif** den Namen Ihrer Bilddatei ein. Wenn Ihre Bilddatei logo.gif heißt, ändern Sie die Zeile zu:

      Unterstützt werden nur Bilddateien im GIF- oder JPG-Format. Lassen Sie die anderen Zeichen in der Zeile unverändert.
5. Speichern Sie die Datei.

Installieren benutzerdefinierter Portalseitendateien

Benutzerdefinierte Portalseiten und die Bilddateien, auf die in den Vorlagen verwiesen wird, müssen auf dem Access Gateway installiert werden.

So wählen Sie eine Portalseite aus

1. Klicken Sie auf der Registerkarte **Portal Page Configuration** auf die Registerkarte **Portal Pages** und dann auf **Add File**.
2. Geben Sie im Feld **File title** den Titel der Datei ein, die Sie hinzufügen.

   Über die Dateititel können Sie die Portalseite leicht mit einer Gruppe verknüpfen. Es kann z. B. vorkommen, dass Sie eine Hauptportalseite haben, die von vielen Gruppen verwendet wird, und eine separate Portalseite, die nur Gästen angezeigt wird. In diesem Fall können Sie die Dateien "Hauptanmeldung" und "Gastanmeldung" nennen. Wenn Sie mehrere Portalseiten haben, die bestimmten Benutzergruppen entsprechen, bieten sich Namen wie "Adminanmeldung", "Studentenanmeldung" oder "IT-Anmeldung" an.
3. Wählen Sie unter **File Type** ein Dateiformat aus.

   Portalseiten müssen HTML-Dateien sein. Bilder, auf die auf einer HTML-Seite verwiesen wird, müssen entweder im GIF- oder im JPG-Format vorliegen.
4. Klicken Sie auf **Upload File**.
5. Gehen Sie zur Datei und klicken Sie auf **Öffnen**.

   Die Datei wird auf das Access Gateway installiert.

So entfernen Sie eine Portaldatei vom Access Gateway

Wählen Sie auf der Registerkarte **Portal Pages** den Seitennamen aus der Liste und klicken Sie auf **Remove Selected File**.

Auswählen einer Portalseite für eine Gruppe

In der Standardeinstellung melden sich alle Benutzer über die Standardportalseite mit dem Access Gateway Plug-in am Access Gateway an oder indem sie das Access Gateway Plug-in auf das Clientgerät herunterladen und installieren. Sie können benutzerdefinierte Portalseiten auf das Access Gateway laden (Informationen hierzu finden Sie unter "Installieren benutzerdefinierter Portalseitendateien" auf Seite 176) und dann für jede Gruppe eine Portalseite auswählen. So können Sie steuern, welche Access Gateway-Clientsoftware für welche Gruppe verfügbar ist.

Hinweis: Das Deaktivieren der Anmeldeseitenauthentifizierung auf der Registerkarte **Global Cluster Policies** überschreibt die Anmeldeseiteneinstellung für alle Gruppen. Weitere Informationen hierzu finden Sie unter "Aktivieren der Anmeldeseitenauthentifizierung" auf Seite 172.

So legen Sie eine Portalseite für eine Gruppe fest

1. Klicken Sie mit der rechten Maustaste auf der Registerkarte **Access Policy Manager** unter **User Groups** auf eine Gruppe und klicken Sie dann auf **Properties**.
2. Klicken Sie auf der Registerkarte **Gateway Portal** unter **Portal configuration** auf **Use custom portal page** und wählen Sie dann die Seite aus und klicken Sie auf **OK**.

Konfigurieren einer Portalseite mit mehreren Anmeldeoptionen

Benutzer können auf einer Webseite die Option haben, sich über das Access Gateway Plug-in oder das Webinterface anzumelden. Diese Portalseite kann im Gegensatz zur Standardportalseite nicht konfiguriert werden. Benutzern werden zwei Symbole angezeigt und sie können dann wählen, mit welchem der folgenden Verfahren sie sich am Access Gateway anmelden möchten. Zur Auswahl stehen:

- **Citrix Access Gateway:** Klicken auf dieses Symbol startet das Access Gateway Plug-in. Nach der Anmeldung des Benutzers wird das Webinterface angezeigt.
- **Citrix XenApp:** Klicken auf dieses Symbol leitet Benutzer zum Webinterface weiter.

Diese Portalseite wird nur dann angezeigt, wenn auf der Registerkarte **Gateway Portal** die Optionen **Redirect to Web Interface** und **Use the multiple logon option page** aktiviert sind.

So konfigurieren Sie mehrere Anmeldeoptionen

1. Klicken Sie mit der rechten Maustaste im linken Bereich der Registerkarte **Access Policy Manager** auf eine Gruppe und klicken Sie dann auf **Properties**.
2. Wählen Sie auf der Registerkarte **Gateway Portal** die Option **Redirect to Web Interface**.
3. Geben Sie im Feld **Path** den Pfad des Servers ein, auf dem das Webinterface gehostet wird.

   Der Standardsitepfad für Citrix Presentation Server 4.2 ist Citrix/MetaFrame/auth/Login.aspx.

   Der Standardsitepfad für Citrix Presentation Server 4.5 ist /Citrix/AccessPlatform.

   Der Standardsitepfad für Citrix XenApp 5.0 ist /Citrix/XenApp.
4. Geben Sie in das Feld **Web server (IP address or FQDN)** die IP-Adresse oder den FQDN des Servers an, auf dem das Webinterface gehostet wird.

5. Wählen Sie **Use a secure connection**, um die Verbindung zu sichern.
6. Um die Anmeldung für das Access Gateway Plug-in bereitzustellen, wählen Sie **Use the multiple logon option page** und klicken Sie auf **OK**.

Hinweis: Das Webinterface muss Verbindungen vom Access Gateway unterstützen, um diese Konfiguration abschließen zu können. Weitere Informationen über die Konfiguration des Webinterface finden Sie in der *Citrix Access Gateway Standard Edition – Integrationsdokumentation für Citrix XenApp und Citrix XenDesktop*.

Anmelden, wenn Vorauthentifizierungsrichtlinien konfiguriert sind

Ist eine Vorauthentifizierungsrichtlinie auf dem Access Gateway konfiguriert, wird das Citrix Prescan Plug-in auf das Clientgerät heruntergeladen und installiert, wenn Benutzer sich über eine Webadresse oder über das Startmenü verbinden. Falls das Clientgerät die Richtlinienüberprüfung vor der Authentifizierung besteht, werden die Benutzer mit der Anmeldeseite verbunden, von wo aus sie sich mit ihren Anmeldeinformationen am Access Gateway anmelden können. Sollte der Vorauthentifizierungsscan fehlschlagen, werden die Benutzer in einer Fehlermeldung aufgefordert, sich mit dem Helpdesk oder dem Systemadministrator in Verbindung zu setzen. Weitere Informationen finden Sie unter "Konfigurieren von Vorauthentifizierungsrichtlinien" auf Seite 135.

Wartung des Access Gateways

In diesem Kapitel werden die Wartungseinstellungen für das Access Gateway und die Tools, mit denen sie konfiguriert werden, beschrieben.

Alle Konfigurationsänderungen werden automatisch übernommen und führen für die mit dem Access Gateway verbundenen Benutzer zu keinerlei Betriebsunterbrechungen. Richtlinienänderungen treten sofort in Kraft. Wenn eine Verbindung gegen eine neue Richtlinie verstößt, wird sie geschlossen.

Dieses Kapitel enthält:

- "Access Gateway-Verwaltungstools"
- "Aktualisieren der Access Gateway-Software"
- "Neuinstallieren der Access Gateway-Software"
- "Speichern und Wiederherstellen der Access Gateway-Konfiguration"
- "Neustarten und Herunterfahren des Access Gateways"
- "Zulassen von ICMP-Verkehr"
- "Konfigurieren persönlicher Firewalls von Drittanbietern"

Access Gateway-Verwaltungstools

Für die Administration von Access Gateway wird eine Kombination von Administration Portal und Administration Tool verwendet, um das Gerät zu verwalten und die Netzwerkverbindungen zu überwachen. Das Administration Tool enthält sämtliche Steuerelemente für die Access Gateway-Konfiguration. Nur das Administratorkonto kann ausschließlich über das Administration Portal und die serielle Konsole verwaltet werden. Im Administration Portal finden Sie Downloads und Sie können einige Access Gateway-Einstellungen verwalten.

Administration Tool

Mit dem Administration Tool können Sie globale Einstellungen konfigurieren und diese dann auf die verschiedenen Access Gateway-Geräte im Netzwerk übertragen. Sie können mit dem Administration Tool außerdem Gerätestatistiken anzeigen und die Netzwerkverwendung überwachen.

Im linken Bereich des Administration Tool-Fensters finden Sie Hilfeinformationen für die aktuell ausgewählte Registerkarte. Die Onlinehilfe passt sich an die Aufgabe an, die Sie gerade ausführen.

Außerdem werden im Bereich **Alerts** über der Onlinehilfe Warnungen angezeigt. Warnungen informieren Sie, wenn auf dem Access Gateway ein Problem aufgetreten ist, z. B. eine fehlende Lizenz oder ein Zertifikat.

Das Administration Tool wird vom Administration Portal aus heruntergeladen und installiert.

Wichtig: Bei einem Upgrade von einer älteren Access Gateway-Version müssen Sie das Administration Tool zunächst über die Systemsteuerung deinstallieren, bevor Sie die neueste Version vom Administration Portal herunterladen und installieren.

So installieren und starten Sie das Administration Tool

1. Klicken Sie im Administration Portal auf **Downloads**.
2. Klicken Sie unter **Access Gateway Administration Tool** auf **Install the Access Gateway Administration Tool** und klicken Sie dann auf **Run**.
3. Folgen Sie den Anweisungen im Installationsassistenten, um das Administration Tool zu installieren.
4. Sie starten das Administration Tool indem Sie auf **Start > Alle Programme > Citrix > Access Gateway Administration Tool 4.6 > Access Gateway Administration Tool 4.6** oder das Symbol auf dem Desktop klicken.
5. Geben Sie im Dialogfeld **Administrator Login** unter **Host (IP or FQDN)** die IP-Adresse des Access Gateways ein.
6. Geben Sie im Feld **Administrator Username** als Benutzernamen **root** ein.
7. Geben Sie im Feld **Administrator Password** das Standardkennwort **rootadmin** oder das neue Kennwort ein, wenn es mit der seriellen Konsole oder dem Administration Portal geändert wurde und klicken Sie auf **Connect**.

Administration für mehrere Versionen von Access Gateway

Wenn Sie in Ihrem Netzwerk mehrere Geräte haben und es sich dabei um verschiedene Versionen handelt, können Sie mehrere Instanzen des Administration Tools auf Ihrem Computer installieren. Mit dem Access Gateway Version 4.6 Administration Tool lassen sich frühere Versionen des Access Gateway-Geräts verwalten. Mit dem Access Gateway Version 4.6 Administration Tool lassen sich frühere Versionen des Access Gateway-Geräts verwalten.

Auf der Registerkarte **Access Gateway Cluster** klicken Sie auf der Registerkarte **Statistics** und dann auf die Registerkarte **System**, um herausfinden, welche Version des Tools Sie verwenden.

Bei Verbindungen zu älteren Versionen des Access Gateways werden neue Features nicht unterstützt. Im Administration Tool werden diese Einstellungen nicht deaktiviert, sondern ohne Warnung ignoriert. Die folgenden Features werden nicht unterstützt, wenn Sie eine Verbindung zu früheren Versionen des Access Gateways herstellen:

Access Gateway Version	Nicht unterstütztes Feature
4.5.5 oder früher	Anwendungsbeschleunigung mit Citrix Branch Repeater aktivieren
4.5.7 oder früher	Zwischenspeichern des falschen Kennworts Load Balancing der anfänglichen Anmeldeanfragen zu Access Gateway Advanced Edition
4.5.8 oder früher	Upgradeaufforderung für frühere Versionen des Gateway Plug-ins Namensänderung von Secure Access Client zu Access Gateway Plug-in

Außerdem werden die Netzwerküberwachungstools, die in Version 4.6 auf der Registerkarte **Access Gateway Cluster** integriert wurden, nicht in früheren Versionen des Access Gateways unterstützt.

Administration Portal

Das Administration Portal bietet eine webbasierte Benutzeroberfläche für Administratoren. Es hat mehrere Registerkarten, die Ihnen die Verwaltung des Access Gateways erleichtern sollen.

So öffnen Sie das Administration Portal

1. Geben Sie in einem Webbrowser https://***AccessGatewayFQDN*:9001/** ein.
2. Geben Sie den Administratorbenutzernamen und das Kennwort ein. Die Standardwerte sind **root** und **rootadmin**.

   Das Administration Portal wird geöffnet. Nachfolgend werden die Tasks beschrieben, die Sie mit dem Administration Portal ausführen können.

Herunterladen von Tools und Dokumentation

Auf der Seite **Downloads** haben Sie folgende Optionen:

- Herunterladen des Administration Tools
- Herunterladen der Access Gateway-Dokumentation
- Herunterladen einer Portalseitenvorlage
- Herunterladen der Muster-E-Mail für Benutzer
- Herunterladen von Access Gateway-spezifischen SNMP-Daten

Konfigurieren des Administratorkennworts

Das Access Gateway verfügt über ein Standardadministratorkonto mit uneingeschränktem Zugriff auf das Gerät. Um das Access Gateway vor unbefugtem Zugriff zu schützen, sollten Sie das Standardkennwort während der Erstkonfiguration ändern. Der Standardbenutzername für den Access Gateway-Administrator ist **root** und das zugehörige Kennwort **rootadmin**. Das Administratorkennwort kann im Administration Portal oder der seriellen Konsole geändert werden. Citrix empfiehlt, dass Sie das Administratorkennwort mit der seriellen Konsole nach der Installation des Geräts ändern. Weitere Informationen hierzu finden Sie unter "Konfigurieren der TCP/IP-Einstellungen mit der seriellen Konsole" auf Seite 36.

Hinweis: Wenn Sie das Standardkennwort für das Administratorkonto auf den Standardwert zurücksetzen möchten, müssen Sie die Access Gateway-Serversoftware neu installieren. Das neue Kennwort darf bis zu 127 Zeichen enthalten. Weder am Anfang noch am Ende darf ein Leerzeichen stehen.

So ändern Sie das Administratorkennwort im Administration Portal

1. Klicken Sie im Administration Portal auf der Registerkarte **Administration** auf **Admin Password**.
2. Geben Sie unter **Administrator Password** das neue Kennwort ein.
3. Klicken Sie auf **Change Password**.

Anzeigen von Protokollinformationen

Auf der Seite **Logging** wird das Protokoll für das Access Gateway angezeigt. Die hier angezeigten Informationen sind mit denen identisch, die im Administration Tool auf der Registerkarte **Access Gateway Cluster > Logging/Settings** angezeigt werden. Sie können außerdem die Buildversion des Access Gateways auf dieser Registerkarte sehen.

Ausführen von Wartungsaufgaben

Auf der Seite **Maintenance** können Sie Verwaltungsaufgaben ausführen. Dazu gehören folgende Einstellungen:

- Hochladen signierter Zertifikate (.crt)
- Hochladen privater Schlüssel und Zertifikate (.pem)
- Eingeben des Kennworts für einen privaten Schlüssel
- Hochladen gespeicherter Konfigurationen oder Upgrades
- Suchen nach Geräteaktualisierungen
- Speichern der Gerätekonfiguration
- Neustarten und Herunterfahren des Geräts

Durch Klicken auf **Log Out** können Sie sich vom Administration Portal abmelden.

Verwalten externer Verbindungen mit dem Administration Portal

Wenn Sie das Access Gateway so konfigurieren, dass beide Netzwerkadapter verwendet werden, kann der externe Adapter standardmäßig für den Zugriff auf das Administration Portal vom Internet aus verwendet werden. Sie können den Zugriff vom Internet auf das Administration Portal blockieren, indem Sie die Option deaktivieren.

So blockieren Sie den externen Zugriff auf das Administration Portal

1. Klicken Sie im Administration Tool auf die Registerkarte **Access Gateway Cluster** und öffnen Sie das Fenster für das Access Gateway.
2. Deaktivieren Sie auf der Registerkarte **Administration** unter **Access management** die Option **Enable external administration**.
3. Klicken Sie auf **Apply Change**.

Aktualisieren der Access Gateway-Software

Die Software auf dem Access Gateway kann bei Veröffentlichung neuer Releases über ein Upgrade aktualisiert werden. Ob neue Aktualisierungen zur Verfügung stehen, erfahren Sie im Administration Portal. Ein Upgrade auf ein neues Release ist nur dann möglich, wenn Ihre Access Gateway-Lizenzen zum Zeitpunkt der Veröffentlichung der Aktualisierung am Subscription Advantage-Programm teilnehmen. Das Subscription Advantage-Abonnement kann jederzeit erneuert werden. Weitere Informationen finden Sie auf der Citrix Support-Website unter http://support.citrix.com.

Wichtig: Das Linux-Betriebssystem für Access Gateway Version 4.6 wurde auf eine neuere Version aktualisiert. Um Version 4.6 auf dem Access Gateway zu installieren, müssen Sie ein neues Image auf das Gerät spielen und dann die Software installieren. Weitere Informationen über das Überspielen eines neuen Images finden Sie unter "Neuinstallieren der Access Gateway-Software" auf Seite 189.

So prüfen Sie, ob neue Softwareaktualisierungen veröffentlicht wurden

1. Öffnen Sie das Administration Portal und klicken Sie auf **Maintenance**.
2. Klicken Sie auf **Check for Server Upgrade**.

   Die Citrix Support-Website wird geöffnet und Sie können, so vorhanden, das Upgrade von der Website herunterladen.

Mit dieser Access Gateway-Version können gespeicherte Konfigurationen früherer Versionen des Geräts gelesen werden. Wenn eine gespeicherte Konfiguration einer früheren Version mit Access Gateway Version 4.6 wiederhergestellt wird, wird sie automatisch in das neue Format konvertiert. Wenn Sie ein Upgrade von einer älteren Version des Access Gateways auf diese Version durchführen, ist es wichtig, die aktuelle Konfiguration vorher zu speichern. Wenn Sie ein Upgrade auf Version 4.6 durchführen und die Konfigurationsdatei speichern, kann diese Datei auf früheren Versionen des Access Gateways nicht mehr verwendet werden. Wenn Sie versuchen, die Konfigurationsdatei aus Version 4.6 auf eine frühere Version hochzuladen, kann das Access Gateway nicht mehr verwendet werden. Wenn Sie eine frühere Version der Software wiederherstellen müssen, müssen Sie ein neues Image auf das Gerät spielen. Nachdem das neue Image auf das Gerät aufgespielt wurde, können Sie die gespeicherte Konfiguration wiederherstellen.

Wichtig: Das Access Gateway hat das Standardadministratorkennwort *rootadmin*. Wenn Sie das Administratorkennwort ändern, müssen Sie ein neues mit mindestens sechs Zeichen wählen.

Wiederherstellen gespeicherter privater Zertifikatschlüssel

Die privaten Schlüssel für mit Access Gateway Version 4.5 oder höher erstellten Zertifikate sind jetzt verschlüsselt und durch Kennwörter geschützt. Die neuen privaten Schlüssel sind nicht mit früheren Versionen der Access Gateway-Software kompatibel. Aus diesem Grund ist es wichtig, vor einem Upgrade die aktuelle Konfiguration zu speichern.

Wenn eine gespeicherte Konfiguration auf dem Gerät wiederhergestellt wird, ist das Kennwort für den privaten Schlüssel nicht erforderlich. Das Kennwort wird auch beim Speichern der Gerätekonfiguration nicht benötigt. Das Kennwort ist beim Installieren oder Erstellen eines Zertifikats mit Access Gateway Version 4.6 erforderlich. Wenn Sie ein neues, mit Version 4.5 erstelltes Zertifikat hochladen oder eine gespeicherte Konfiguration einer früheren Version der Software wiederherstellen, werden Sie zur Eingabe des Kennworts aufgefordert. Wenn der private Schlüssel des Zertifikats verschlüsselt ist, kann der Schlüssel mit dem Kennwort entschlüsselt werden. Wenn der private Schlüssel nicht verschlüsselt ist, wird er mit dem Kennwort verschlüsselt. Wenn Sie ein Upgrade von einer früheren Version des Access Gateways durchführen und der private Schlüssel kein Kennwort hat, wird ein zufällig erstelltes Kennwort zugewiesen und der private Schlüssel wird damit verschlüsselt.

Installieren des Software-Upgrades

Zum Hochladen der neuen Software auf das Gerät steht Ihnen das Administration Tool zur Verfügung. Lesen Sie sich vor der Installation des Upgrades die Dokumentation zur Software durch.

Hinweis: Wenn Sie ein Serverupgrade hochladen, beendet das Access Gateway alle aktiven Sitzungen. Es empfiehlt sich daher, Upgrades möglichst dann durchzuführen, wenn der Netzwerkverkehr eher gering ist.

So laden Sie ein Upgrade auf das Access Gateway hoch

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Access Gateway.
2. Klicken Sie auf die Registerkarte **Administration**.
3. Klicken Sie unter **Upgrade and configuration management** neben **Upload an upgrade or saved configuration** auf **Browse**.
4. Suchen Sie die Upgradedatei, die hochgeladen werden soll, und klicken Sie auf **Öffnen**.

   Die Datei wird hochgeladen und Sie werden zum Neustart des Access Gateways aufgefordert.

Hinweis: Sie können die Access Gateway-Software auch über die Seite **Maintenance** im Administration Portal aktualisieren.

Wenn Sie das Access Gateway aktualisieren, werden alle Ihre Konfigurationseinstellungen gespeichert. Informationen zum Speichern und Wiederherstellen einer Konfiguration finden Sie unter "Speichern und Wiederherstellen der Access Gateway-Konfiguration" auf Seite 192.

Neuinstallieren der Access Gateway-Software

Wenn Sie eine vollständige Neuinstallation der Access Gateway-Software durchführen, können Sie dafür die Originalsoftware verwenden, die mit dem Geräte geliefert wurde. Sollen die Konfigurationseinstellungen erhalten bleiben, müssen Sie vor der Neuinstallation der Software ein Backup der Konfiguration erstellen.

Neuinstallation der Software bei Model 2000

Bei Access Gateway Model 2000 verwenden Sie die Restore-CD, um die Software neu zu installieren.

So installieren Sie die Access Gateway-Serversoftware auf Model 2000

1. Speichern Sie die Access Gateway-Konfigurationseinstellungen wie unter "Speichern und Wiederherstellen der Access Gateway-Konfiguration" auf Seite 192 beschrieben.
2. Stellen Sie sicher, dass das Access Gateway mit einem Computer verbunden ist, auf dem die Terminalemulationssoftware ausgeführt werden kann. Schalten Sie beide Systeme ein.
3. Legen Sie die Access Gateway Restore-CD in das CD-Laufwerk des Access Gateways ein, um das Installationsprogramm zu starten.

   Wenn die Installation abgeschlossen ist, zeigt die serielle Konsole eine entsprechende Meldung an.
4. Nehmen Sie die Restore-CD wieder heraus und schalten Sie das Access Gateway aus.
5. Schalten Sie das Access Gateway ein.
6. Stellen Sie die Konfigurationseinstellungen wieder her. Informationen hierzu finden Sie unter "Speichern und Wiederherstellen der Access Gateway-Konfiguration" auf Seite 192.

Neuinstallation der Software bei Model 2010

Bei Model 2010 wird die Access Gateway-Software über einen USB-Stick installiert. Die Software wird auf den Windows-Computer heruntergeladen und dann auf den USB-Stick kopiert. Sie stecken den USB-Stick in das Access Gateway ein und installieren die Software neu.

Achtung: Beim Kopieren der Access Gateway-Software auf den USB-Stick werden alle ggf. auf dem USB-Stick vorhandenen Daten gelöscht. Achten Sie daher darauf, dass auf dem USB-Stick keine wichtigen Daten sind. Wenn Sie den Windows-Computer oder das Access Gateway neu starten, während der USB-Stick angeschlossen ist, wird versucht, auf den Computer oder das Access Gateway ein neues Image aufzuspielen.

Systemvoraussetzungen

Um ein Installationspaket auf einem USB-Stick zu erstellen, brauchen Sie Folgendes:

- 1 GB USB-Stick
- .NET Framework 1.0
- Eines der folgenden Windows-Betriebssysteme muss installiert sein:
  - Windows 2000 Server
  - Windows 2000 Professional
  - Windows Server 2003
  - Windows XP
  - Windows Vista
- USB-Port auf dem Windows-Computer
- Access Gateway-CD
- Appliance Software Imaging Tool, das Sie von der Citrix Support-Website erhalten.

Hinweis: Access Gateway Model 2010 unterstützt nur Version 4.5.5 oder höher der Access Gateway-Software.

So installieren Sie die Access Gateway-Serversoftware auf Model 2010

1. Speichern Sie die Access Gateway-Konfigurationseinstellungen wie unter "Speichern und Wiederherstellen der Access Gateway-Konfiguration" auf Seite 192 beschrieben.
2. Stellen Sie sicher, dass das Access Gateway mit einem Computer verbunden ist, auf dem die Terminalemulationssoftware ausgeführt werden kann. Schalten Sie beide Systeme ein.

3. Laden Sie die Access Gateway-Software von der Citrix Support-Website auf Ihren Computer und kopieren Sie dann das Image auf einen USB-Stick. Verwenden Sie dazu das Appliance Software Imaging Tool, das Sie auch auf der Support-Website erhalten.

   Achtung: Nachdem Sie die Access Gateway-Software auf den USB-Stick kopiert haben, sollten Sie sofort die Access Gateway-CD aus dem Computer entfernen. Wenn Sie den Computer neu starten, während der USB-Stick angeschlossen oder die CD eingelegt ist, werden möglicherweise die Informationen auf Ihrem Computer gelöscht.

4. Stecken Sie den USB-Stick in den USB-Port auf dem Access Gateway, um das Installationsprogramm zu starten.

   Wenn die Installation abgeschlossen ist, zeigt die serielle Konsole eine entsprechende Meldung an.

5. Entfernen Sie den USB-Stick und schalten Sie das Access Gateway aus.
6. Schalten Sie das Access Gateway ein.
7. Stellen Sie die Konfigurationseinstellungen wieder her. Informationen hierzu finden Sie unter "Speichern und Wiederherstellen der Access Gateway-Konfiguration" auf Seite 192.

Speichern und Wiederherstellen der Access Gateway-Konfiguration

Wenn Sie das Access Gateway aktualisieren, werden alle Ihre Konfigurationseinstellungen, einschließlich der hochgeladenen Zertifikate, Lizenzen und Portalseiten, automatisch wiederhergestellt. Wenn Sie die Access Gateway-Software jedoch neu installieren, müssen Sie Ihre Konfigurationseinstellungen manuell speichern und dann wiederherstellen.

Hinweis: Zum Speichern und Wiederherstellen der Konfigurationseinstellungen steht Ihnen auch die Registerkarte **Maintenance** des Administration Portals zur Verfügung.

So speichern Sie die Access Gateway-Konfiguration

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Access Gateway.
2. Klicken Sie auf der Registerkarte **Administration** im Bereich **Upgrade and configuration management** neben **Save the current configuration** auf **Save Configuration**.
3. Speichern Sie die Datei **config.restore** auf Ihrem Computer.

Daraufhin wird die gesamte Access Gateway-Konfiguration gespeichert, einschließlich der Systemdateien, installierten Lizenzen und installierten Serverzertifikate.

Nach der Installation der Access Gateway-Software können Sie die gespeicherte Konfiguration wiederherstellen.

So stellen Sie eine gespeicherte Konfiguration wieder her

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Access Gateway.
2. Klicken Sie auf der Registerkarte **Administration** im Bereich **Upgrade and configuration management** neben **Upload an upgrade or saved configuration** auf **Browse**.
3. Suchen Sie die Datei config.restore und klicken Sie auf **Öffnen**.

   Nachdem die Konfigurationsdatei hochgeladen wurde, starten Sie das Access Gateway neu und alle Konfigurationseinstellungen, Lizenzen und Zertifikate werden wiederhergestellt.

Wenn Sie die RSA SecurID-Authentifizierung verwenden, müssen Sie das Node Secret auf dem RSA ACE/Server zurücksetzen (siehe dazu "Zurücksetzen des Node Secrets" auf Seite 98). Da die Access Gateway-Einstellungen wiederhergestellt wurden, ist das Node Secret nicht mehr auf dem Gerät, sodass jeder Versuch einer RSA ACE/Server-Authentifizierung scheitert, bis das Node Secret zurückgesetzt wurde.

Neustarten und Herunterfahren des Access Gateways

Sie können das Access Gateway entweder über das Administration Portal oder das Administration Tool neu starten oder herunterfahren.

Neustarten des Access Gateways

Wenn Sie Änderungen am Access Gateway vorgenommen haben, müssen Sie das Gerät u. U. neu starten.

So starten Sie das Access Gateway neu

1. Klicken Sie im Administration Tool auf die Registerkarte **Access Gateway Cluster** und öffnen Sie das Fenster für das Access Gateway.
2. Klicken Sie auf der Registerkarte **Administration** im Bereich **Access Gateway management** neben **Restart the appliance** auf **Restart**.

   - Oder -

   Klicken Sie im Menü **Action** auf **Restart** ***Access Gateway-Name***, wobei *Access Gateway-Name* der Name des Geräts ist.

Sie können Access Gateway auch über das Administration Portal neu starten.

So starten Sie das Access Gateway über das Administration Portal neu

Klicken Sie auf der Registerkarte **Maintenance** neben **Restart the server** auf **Restart**.

Herunterfahren des Access Gateways

Fahren Sie das Access Gateway niemals herunter, indem Sie den Netzschalter drücken. Verwenden Sie die Befehle im Administration Tool oder im Administration Portal zum Herunterfahren des Geräts. Der Netzschalter darf nur zum Einschalten des Geräts verwendet werden.

So fahren Sie das Access Gateway herunter

1. Klicken Sie im Administration Tool auf die Registerkarte **Access Gateway Cluster** und öffnen Sie das Fenster für das Access Gateway.
2. Klicken Sie auf der Registerkarte **Administration** im Bereich **Access Gateway management** neben **Shut down the appliance** auf **Shut down**.

   - Oder -

   Klicken Sie im Menü **Action** auf **Shut down *Access Gateway-Name***, wobei *Access Gateway-Name* der Name des Geräts ist.

Das Access Gateway kann auch mit dem Administration Portal heruntergefahren werden.

So fahren Sie das Access Gateway über das Administration Portal herunter

Klicken Sie auf der Registerkarte **Maintenance** neben **Shut down the server** auf **Shut down**.

Initialisieren des Access Gateways

Nach dem Ändern der Verwaltungseinstellungen müssen Sie das Access Gateway initialisieren, damit die Änderungen wirksam werden. Wenn die Initialisierung des Access Gateways erforderlich ist, wird im Administration Tool im Bereich **Alerts** eine Meldung angezeigt.

Beim Initialisieren des Access Gateways werden alle Benutzer vom Access Gateway getrennt. Sie sollten die Initialisierung daher zu Zeiten durchführen, wenn möglichst wenige Benutzer mit dem Access Gateway verbunden sind.

So initialisieren Sie das Access Gateway

Klicken Sie auf der Registerkarte **Administration** im Bereich **Access Gateway management** neben **Initialize the appliance** auf **Initialize**.

- Oder -

Klicken Sie im Menü **Action** auf **Initialize *Access Gateway-Name***, wobei *Access Gateway-Name* der Name des Geräts ist.

Zulassen von ICMP-Verkehr

ICMP-Verkehr (Internet Control Message Protocol) zum Access Gateway ist standardmäßig deaktiviert. Wenn Sie ICMP-Verkehr zulassen möchten, verwenden Sie die Registerkarte **Access Gateway Cluster > Administration**.

Wenn ICMP-Verkehr zugelassen ist, können die Benutzer Server im internen, sicheren Netzwerk "pingen". Das Access Gateway selbst kann keinen ICMP-Verkehr empfangen.

So lassen Sie ICMP-Verkehr zu

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Access Gateway.
2. Wählen Sie auf der Registerkarte **Administration** unter **Access management** die Option **Allow ICMP traffic** und klicken Sie auf **Apply Change**.

Konfigurieren persönlicher Firewalls von Drittanbietern

Wenn ein Benutzer keine Verbindung zum Access Gateway herstellen oder nicht auf zugelassene Ressourcen zugreifen kann, wird der Verkehr möglicherweise durch die Firewallsoftware auf dem Computer des Benutzers blockiert. Das Access Gateway kann zusammen mit allen persönlichen Firewalls eingesetzt werden, sofern für das Access Gateway ein vertrauenswürdiges Netzwerk oder eine vertrauenswürdige IP-Adresse angegeben werden kann.

Citrix empfiehlt, dass die persönlichen Firewalls der Benutzer Vollzugriff für das Citrix Access Gateway Plug-in zulassen. Wenn Sie keinen vollständigen Zugriff gewähren möchten, sollten die folgenden UDP- und UDP/TCP-Ports auf dem Clientgerät offen sein:

- 10000 (UDP)
- 10010 (UDP/TCP)
- 10020 (UDP)
- 10030 (UDP)

Persönliche Firewalls müssen so konfiguriert sein, dass sie eingehenden und ausgehenden Datenverkehr von der IP-Adresse oder dem vollqualifizierten Domänennamen des Access Gateways zulassen. In den Access Gateway Plug-in-Eigenschaften sehen Sie, welche Ports offen sind. Sie öffnen die Eigenschaften über das Verbindungssymbol im Infobereich. Die offenen Ports werden auf der Registerkarte **Details** aufgeführt.

Wenn Sie das Access Gateway Plug-in auf einem Clientgerät ohne Administratorrechte installieren, können Benutzer die Firewallregeln nicht ändern, um den Zugriff zuzulassen. Benutzer müssen mit Administratorrechten angemeldet sein, um die Firewallregeln zu ändern. Bei Clientgeräten mit Windows Firewall versucht das Installationsprogramm für das Access Gateway Plug-in automatisch, eine Ausnahme für die Firewallregeln hinzuzufügen. Wenn das Clientgerät eine Firewall von Drittanbietern verwendet, müssen Sie die Ports manuell konfigurieren.

So zeigen Sie die Access Gateway Plug-in-Statuseigenschaften an

Doppelklicken Sie im Infobereich auf das Access Gateway-Verbindungssymbol. Sie können stattdessen auch mit der rechten Maustaste auf das Symbol klicken und im Kontextmenü den Befehl **Eigenschaften** wählen.

Das **Citrix Access Gateway**-Dialogfeld wird angezeigt.

Die Verbindungseigenschaften enthalten nützliche Informationen für die Problembehandlung. Hierzu gehören z. B. folgende Eigenschaften:

- Die Registerkarte **Allgemein** enthält Verbindungsinformationen.
- Auf der Registerkarte **Details** finden Sie Serverinformationen und eine Liste der gesicherten Netzwerke, auf die Benutzer zugreifen können.
- Die Registerkarte **Zugriffslisten** enthält die Zugriffssteuerungslisten (ACLs), die für die Benutzerverbindung konfiguriert sind. Diese Registerkarte wird nur für Benutzer angezeigt, die Mitglied einer Gruppe sind. Wenn für eine Gruppe keine Zugriffssteuerungsliste konfiguriert ist, wird die Registerkarte auch nicht angezeigt.

Im Folgenden finden Sie Vorschläge für Firewalls, die häufig mit dem Access Gateway eingesetzt werden.

Hinweis: Vollständige Anweisungen zur Konfiguration der Firewalls finden Sie in der Herstellerdokumentation.

McAfee Personal Firewall Plus

Mit den McAfee Personal Firewall Plus-Einstellungen kann das Access Gateway Plug-in eine Verbindung zum Internet und den vom Access Gateway zugelassenen Ressourcen herstellen.

Bei den Einstellungen wird davon ausgegangen, dass als Sicherheitsstufe die Einstellung Standardsicherheit ausgewählt ist. Stellen Sie sicher, dass die IP-Adresse oder der IP-Adressbereich der zugelassenen Ressourcen als vertrauenswürdige IP-Adressen hinzugefügt wurden. Wählen Sie in der Liste der Systemdienste alle Dienste aus, die über die VPN-Verbindung verwendet werden sollen.

Hinweis: Wenn das Access Gateway Plug-in installiert ist, werden Sie standardmäßig von Personal Firewall Plus aufgefordert, den Zugriff für diese Anwendung zu gewähren oder zu sperren. Wählen Sie Zugriff gewähren.

Norton Personal Firewall

Bei Norton Personal Firewall mit den Standardeinstellungen können Sie einfach auf die Warnmeldungen reagieren, wenn Sie das erste Mal versuchen, das Access Gateway Plug-in zu starten, oder wenn Sie auf einen gesperrten Speicherort oder eine gesperrte Anwendung zugreifen. Wenn Sie auf solche Warnmeldungen reagieren, können Sie festlegen, ob die Aktion immer zugelassen oder verhindert werden soll. Sie sollten die Aktion immer verhindern.

Sygate Personal Firewall (kostenlose und Pro-Version)

Jedes Mal, wenn die Sygate Personal Firewall auf eine neue Aktivität stößt, für die es noch keine Regel gibt, wird eine Eingabeaufforderung angezeigt. Gewähren Sie Zugriff auf die Anwendungen und Speicherorte, auf die Sie mit dem Access Gateway Plug-in zugreifen möchten. Klicken Sie auf **Ja**, wenn eine Aufforderung angezeigt wird.

Tiny Personal Firewall

Mit den Tiny Personal Firewall-Einstellungen kann das Access Gateway Plug-in eine Verbindung zum Internet und den vom Access Gateway zugelassenen Ressourcen herstellen. Um die Einstellungen zu konfigurieren, öffnen Sie das Verwaltungsfenster der Tiny Personal Firewall und ändern Sie die Einstellungen für die Filterregeln.

Hinweis: Eine Methode zum Konfigurieren der Tiny Personal Firewall besteht darin, auf die Eingabeaufforderungen zu reagieren, die angezeigt werden, wenn die Firewall auf eine neue Aktivität stößt, für die es noch keine Regel gibt. Konfigurieren Sie Tiny Personal Firewall bevor Sie das Access Gateway Plug-in installieren.

Nachdem Sie die Konfigurationsänderungen angewendet und das Access Gateway Plug-in gestartet haben, zeigt Tiny Personal Firewall mehrere Warnungen über eingehende Verbindungen im Zusammenhang mit dem Access Gateway Plug-in. Sie sollten für jede Warnung die Verbindung zulassen.

ZoneAlarm Pro

Damit das Access Gateway Plug-in Client eine Verbindung zum Internet und den vom Access Gateway zugelassenen Ressourcen herstellen kann, müssen Sie den vollqualifizierten Domänennamen des Geräts als vertrauenswürdige Zone hinzufügen.

Installieren zusätzlicher Access Gateway-Geräte

Sie können in Ihrem Netzwerk mehrere Access Gateway-Geräte installieren. Die zusätzlichen Geräte können sich dabei in einem Cluster oder hinter einem Load Balancer befinden oder für das Failover auf ein anderes Access Gateway im Netzwerk konfiguriert sein.

Wenn Access Gateway-Geräte in einem Cluster angeordnet sind, haben alle dieselben Einstellungen für den Benutzerzugriff auf die internen Netzwerkressourcen. Benutzer können sich mit jedem Access Gateway-Gerät im Cluster verbinden und erhalten die gleichen Zugriffsberechtigungen auf interne Netzwerkressourcen.

Mit der Installation mehrerer Access Gateway-Geräte können Sie Folgendes erreichen:

- **Skalierbarkeit:** Überschreitet die Anzahl der Benutzer die Kapazität eines einzelnen Access Gateways, können Sie zusätzliche Geräte installieren und so die Arbeitsbelastung bewältigen.
- **Hohe Verfügbarkeit (Failover):** Sie können mehrere Geräte installieren, sodass in jedem Fall ein Access Gateway für die Verbindungen verfügbar ist, wenn ein anderes Access Gateway ausfällt. Diese Konfiguration gewährt eine hohe Verfügbarkeit des internen Netzwerks für die Remotebenutzer.

Um sowohl Skalierbarkeit als auch Failover zu unterstützen, stellen Sie vor den Access Gateway-Geräten einen Load Balancer bereit. Ein Load Balancer eignet sich in der Regel für größere Unternehmen mit zahlreichen Remotebenutzern. Weitere Informationen hierzu finden Sie unter "Konfigurieren mehrerer Geräte für die Verwendung eines Load Balancers" auf Seite 206.

Soll nur Failover unterstützt werden, können Sie zwei (oder mehrere) Access Gateway-Geräte bereitstellen und dann ein Gerät mit dem Administration Tool so konfigurieren, dass dieses Gerät das Failover auf bis zu drei weitere Geräte ausführt. Wenn ein Access Gateway ausfällt, werden die Benutzer automatisch mit einem anderen Access Gateway verbunden. Bei dieser Form der Bereitstellung ist kein Load Balancer erforderlich. Weitere Informationen hierzu finden Sie unter "Konfigurieren von Access Gateway-Failover" auf Seite 212.

Beim Konfigurieren von Lastausgleich und Failover können Sie wahlweise weitere Geräte in den Cluster aufnehmen; dies ist jedoch nicht zwingend erforderlich.

In diesem Kapitel wird vorausgesetzt, dass Sie die folgenden Aufgaben bereits erledigt haben:

- Sie haben auf jedem Access Gateway die TCP/IP-Einstellungen auf der Registerkarte **General Networking** konfiguriert.
- Sie haben auf einem Access Gateway im Netzwerk eine Lizenz installiert (dem *Lizenzserver*).

  Ein Access Gateway im Netzwerk kann als Lizenzserver fungieren. Die Lizenz ist auf einem der Geräte installiert. Die anderen Geräte sind so konfiguriert, dass sie ihre Lizenzen vom Lizenzserver abrufen.
- Sie haben die anderen Geräte so konfiguriert, dass sie eine Verbindung zum Lizenzserver herstellen und die notwendigen Lizenzen abrufen.

  Die anderen im Netzwerk installierten Geräte können auch dann Lizenzen abrufen, wenn sie nicht zum Cluster gehören. Weitere Informationen zur Lizenzierung finden Sie unter "Installieren von Lizenzen" auf Seite 43.
- Sie haben auf jedem Access Gateway ein signiertes, sicheres Zertifikat von einer Zertifizierungsstelle installiert.

  Jedes Gerät im Cluster muss einen eindeutigen vollqualifizierten Domänennamen (FQDN) haben. Werden die Geräte in einem Cluster hinter einem Load Balancer bereitgestellt, muss auf jedem Gerät dasselbe SSL-Serverzertifikat mit demselben FQDN installiert sein. Falls die Geräte in einem Cluster für Failover konfiguriert sind (ohne sich hinter einem Load Balancer zu befinden), muss auf jedem Gerät ein eindeutiges SSL-Serverzertifikat installiert sein.

- Wenn die Geräte im Cluster angeordnet sind, konfigurieren Sie die Einstellungen für mindestens ein Gerät im Netzwerk mit den folgenden Registerkarten im Administration Tool:
  - Access Policy Manager
  - **Authentication**, **Global Cluster Policies**
  - Portal Page Configuration
  - Group Priority

Erstellen eines Clusters mit Access Gateway-Geräten

Wenn Sie mehrere Geräte im Netzwerk nutzen und jedes Gerät dieselben Einstellungen verwendet, können Sie einen Cluster erstellen. Die Einstellungen, die veröffentlicht werden können, werden auf einem Access Gateway konfiguriert und dann für die anderen Geräte veröffentlicht. Alle Geräte im Cluster werden im Administration Tool auf der Registerkarte **Access Gateway Cluster** aufgeführt. Hierdurch lassen sich Konfiguration und Wartung der Geräte im Netzwerk schnell und einfach erledigen.

Die Einstellungen auf der Registerkarte **Access Gateway Cluster** gelten für einzelne Access Gateway-Geräte. Diese Einstellungen werden nicht an das Cluster veröffentlicht. Dazu gehören folgende Einstellungen:

- Allgemeine Netzwerkeinstellungen (Registerkarte General Networking)
- Protokollierung (Registerkarte Logging)
- Verwaltung (Registerkarte Administration)
- Zertifikate (Registerkarte Certificates)
- Lizenzierung (Registerkarte Licensing)
- Routen (Registerkarte Routes)
- Namensdienstanbieter
- Failover (Registerkarte Failover)
- Datum und Uhrzeit (Registerkarte Date)
- Statistiken

Die Einstellungen auf den folgenden Registerkarten im Administration Tool werden auf jedem Gerät im Cluster veröffentlicht.

- Access Policy Manager
- Authentifizierung
- Global Cluster Policies
- Portal Page Configuration
- Group Priority

Durch die Veröffentlichung dieser Einstellungen auf den anderen Geräten ist sichergestellt, dass alle Geräte im Cluster dieselben Einstellungen für die Zugriffskontrolle auf die internen Netzwerkressourcen aufweisen.

Hinweis: Alle Access Gateway-Geräte im Cluster müssen die gleiche Version verwenden. Wenn Sie beispielsweise auf einem Gerät Version 4.6 installieren, müssen auch alle anderen Geräte Version 4.6 verwenden

---

Bevor Sie jedes Gerät dem Cluster hinzufügen, wird das Access Gateway wie unter "Erstmalige Installation des Access Gateways" auf Seite 33 beschrieben installiert und dann das Gerät dem Cluster hinzugefügt.

Wichtig: Für jedes Gerät im Cluster muss dasselbe Administratorkennwort verwendet werden. Access Gateways mit einem abweichenden Administratorkennwort können nicht im Cluster verwaltet werden. Citrix empfiehlt, das Administratorkennwort während der Installation des Access Gateways mit der seriellen Konsole zu ändern. Weitere Informationen finden Sie unter "Konfigurieren der TCP/IP-Einstellungen mit der seriellen Konsole" auf Seite 36 und "Konfigurieren des Administratorkennworts" auf Seite 184. Das Administratorkennwort kann zwischen 6 und 127 Zeichen lang sein. Kennwörter dürfen nicht mit einem Leerzeichen beginnen oder enden.

So fügen Sie dem Cluster Geräte hinzu

1. Öffnen Sie das Administration Tool auf dem primären Access Gateway.
2. Klicken Sie auf die Registerkarte **Access Gateway Cluster**.
3. Geben Sie unter **Add an Access Gateway to the Cluster** in das Feld **FQDN** den vollqualifizierten Domänennamen für ein zusätzliches Access Gateway ein und klicken Sie auf **Add**.
4. Wiederholen Sie Schritt1 bis3 für alle Geräte im Cluster.

Sobald Sie alle Geräte in den Cluster aufgenommen haben, können Sie die Einstellungen vom primären Access Gateway im Cluster veröffentlichen.

So veröffentlichen Sie die Einstellungen von einem Gerät auf den anderen Geräten im Cluster

1. Klicken Sie im Administration Tool auf dem ersten installierten Access Gateway (dem primären Gerät) auf die Registerkarte **Publish**.
2. Klicken Sie auf **Publish**. Die Einstellungen des ersten Access Gateways werden auf allen Access Gateway-Geräten im Cluster veröffentlicht.
3. Klicken Sie auf die Registerkarte **Access Gateway Cluster** und anschließend auf die Registerkarte **Administration**.
4. Klicken Sie im Bereich **Access Gateway management** neben **Restart the appliance** auf **Restart**.

Nach der Veröffentlichung der Konfigurationseinstellungen auf allen Geräten im Cluster müssen alle Access Gateway-Geräte neu gestartet werden, damit die Änderungen in Kraft treten.

Jedes Access Gateway im Cluster wird auf der Registerkarte **Publish** aufgeführt. Im Feld **Synchronization Status** wird für jedes Gerät eine der folgenden Synchronisierungsmeldungen angezeigt:

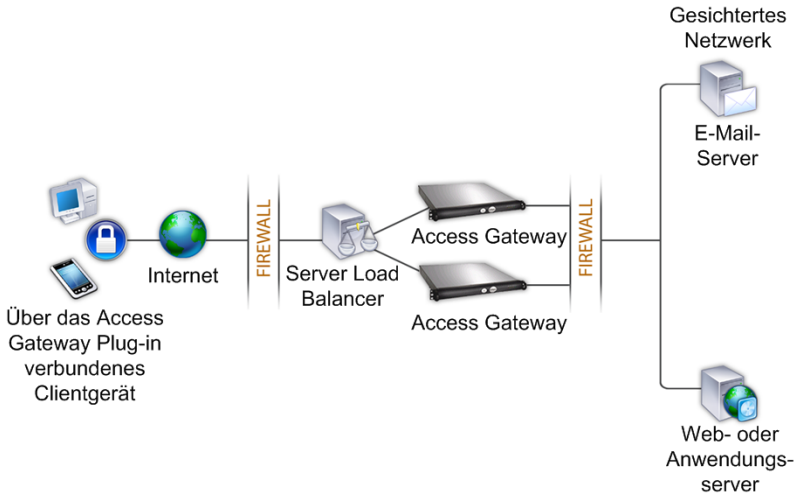
- **In Sync:** Die Access Gateway-Konfiguration wurde erfolgreich veröffentlicht.
- **Not in Sync:** Die Einstellungen wurden geändert, aber nicht veröffentlicht.
- **Sync Failed:** Die Synchronisierung des Access Gateways ist fehlgeschlagen. Überprüfen Sie das Gerät und versuchen Sie es dann noch einmal.
- **Unknown Status:** Der Status des Access Gateways kann nicht ermittelt werden. Überprüfen Sie das Gerät und versuchen Sie es dann noch einmal.

Konfigurieren mehrerer Geräte für die Verwendung eines Load Balancers

Durch die Bereitstellung mehrerer Geräte hinter einem Load Balancer können Sie eine große Anzahl Remotebenutzer unterstützen und dabei die hohe Verfügbarkeit des internen Netzwerks für die Benutzer sicherstellen.

Der Load Balancer, den Sie mit den Geräten bereitstellen, müssen Load Balancing basierend auf Quell-IP (Src IP) unterstützen.

.



Mehrere Access Gateway-Geräte hinter einem Load Balancer

Der Load Balancer ist mit einer eindeutigen IP-Adresse oder einem eindeutigen vollqualifizierten Domänennamen konfiguriert. Diese Adresse wird vom Citrix Access Gateway Plug-in oder einem Webbrowser verwendet, um eine Verbindung zum Load Balancer herzustellen. Der Load Balancer verteilt die Clientverbindungen gleichmäßig auf die Geräte, die hinter ihm bereitgestellt sind.

Sobald eine Clientverbindung eingeht, wählt der Load Balancer mit einem Algorithmus eines der Geräte in der Liste aus und leitet die Clientverbindung an das ausgewählte Access Gateway weiter.

Neben der gleichmäßigen Verteilung der Clientverbindungen trägt ein Load Balancer auch zur hohen Verfügbarkeit des internen Netzwerks bei.

Einige Load Balancer sind in der Lage, den Ausfall von Geräten zu erkennen, die sich hinter ihnen befinden. Wenn ein Load Balancer erkennt, dass ein Gerät ausgefallen ist, entfernt der Load Balancer das betreffende Gerät aus der Liste der verfügbaren Geräte und leitet die Clientverbindungen an die verbleibenden aktiven Geräte um. Sobald das Access Gateway wieder online ist, wird es durch den Load Balancer wieder in die Liste der aktiven Geräte aufgenommen. So wird sichergestellt, dass alle Clientverbindungen auch dann ununterbrochen Zugriff auf das interne Netzwerk erhalten, wenn ein Access Gateway ausfällt.

Konfigurieren des Lastausgleichs

Installieren und konfigurieren Sie den Load Balancer gemäß der Dokumentation des Herstellers in der DMZ des Netzwerks.

Die folgenden Konfigurationsschritte sind erforderlich, damit der Load Balancer mit den Access Gateway-Geräten zusammenarbeitet:

- Konfigurieren Sie den Load Balancer so, dass das Load Balancing der Verbindungen zum Access Gateway-Gerät anhand der Quell-IP durchgeführt wird.
- Konfigurieren Sie den Load Balancer mit einem vollqualifizierten Domänennamen, den das Access Gateway beim Aufbauen der Verbindung zum Load Balancer verwenden soll.
- Konfigurieren Sie den Load Balancer so, dass die SSL-Verschlüsselung nicht beendet wird. Die SSL-Verbindung muss an das Access Gateway übergeben werden; dort erst darf die SSL-Verschlüsselung beendet werden.

Konfigurieren von Access Gateway-Geräten für den Betrieb hinter einem Load Balancer

Im Anschluss an die Installation und Konfiguration des Load Balancers gehen Sie bei den Access Gateway-Geräten, die sich hinter dem Load Balancer befinden, wie folgt vor:

- Schließen Sie für jedes Access Gateway die Netzwerkkabel so an, dass das Interface 0 mit dem Load Balancer verbunden ist und das Interface 1 mit dem internen Netzwerk.
- Konfigurieren Sie die Access Gateway-Geräte hinter dem Load Balancer für den Betrieb als Cluster. Mit einem Cluster stellen Sie sicher, dass alle Access Gateway-Geräte so konfiguriert sind, dass sie den Zugriff auf die Netzwerkressourcen auf dieselbe Weise unterstützen. Über den Load Balancer können Benutzer mit jedem Access Gateway im Cluster eine Verbindung herstellen und erhalten dabei jeweils dieselben Zugriffsrechte. Weitere Informationen hierzu finden Sie unter "Erstellen eines Clusters mit Access Gateway-Geräten" auf Seite 203.
- Erstellen Sie ein einzelnes SSL-Serverzertifikat im PEM-Format und den zugehörigen privaten Schlüssel und laden Sie dieses Zertifikat und den Schlüssel auf alle Access Gateway-Geräte hoch. Weitere Informationen hierzu finden Sie unter "Erstellen eines Zertifikats für Geräte hinter einem Load Balancer" auf Seite 208.

Erstellen eines Zertifikats für Geräte hinter einem Load Balancer

Wenn Sie Access Gateway-Geräte hinter einem Load Balancer bereitstellen, müssen dasselbe SSL-Serverzertifikat und derselbe private Schlüssel auf jedem einzelnen Gerät zur Verfügung gestellt werden.

Wichtig: Erstellen Sie die SSL-Serverzertifikatsanforderung nicht mit der Funktion **Certificate Signing Request** auf der Registerkarte **Access Gateway Cluster** im Administration Tool. Diese Funktion erzeugt einen eigenen privaten Schlüssel auf dem Access Gateway, auf dem sie ausgeführt wird. Wenn Access Gateway-Geräte hinter einem Load Balancer bereitgestellt sind, muss jedes Access Gateway denselben privaten Schlüssel und dasselbe SSL-Zertifikat verwenden.

So erstellen Sie ein SSL-Serverzertifikat und einen privaten Schlüssel

1. Erstellen Sie die SSL-Serverzertifikatsanforderung und den privaten Schlüssel mit einem OpenSSL-Tool, beispielsweise mit Keytool. (Weitere Informationen zu OpenSSL und den verfügbaren Tools finden Sie im Internet unter http://www.openssl.org/.)

   - Erstellen Sie die Serverzertifikatsanforderung im PEM-Format.
   - Verwenden Sie beim Erstellen der Serverzertifikatsanforderung den FQDN des Load Balancers als Servernamen. Verwenden Sie nicht den FQDN einer der Access Gateway-Geräte in der Anforderung.

     Optional können Sie ein Sternchen für den Servernamen im FQDN verwenden, den Sie in der Serverzertifikatsanforderung angeben. Erstellen Sie beispielsweise eine SSL-Serverzertifikatsanforderung für einen Servernamen in diesem Format:

     *.domäne.com
   - Erstellen Sie den privaten Schlüssel getrennt von der Serverzertifikatsanforderung.

2. Senden Sie die SSL-Serverzertifikatsanforderung zum Signieren an eine Zertifizierungsstelle. Senden Sie nur die Serverzertifikatsanforderung im PEM-Format. Senden Sie nicht den privaten Schlüssel.
3. Sobald Sie die signierte SSL-Serverzertifikatsanforderung von der Zertifizierungsstelle erhalten, tragen Sie den privaten Schlüssel manuell oben im signierten Zertifikat ein. Weitere Informationen zum Eintragen eines privaten Schlüssels in ein signiertes Zertifikat finden Sie unter "Kombinieren des privaten Schlüssels mit dem signierten Zertifikat" auf Seite 237.

4. Laden Sie das SSL-Serverzertifikat und den privaten Schlüssel auf alle Access Gateway-Geräte hinter dem Load Balancer hoch.

   A. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Access Gateway.

   B. Klicken Sie auf die Registerkarte **Administration**.

   C. Klicken Sie unter **Secure certificate management** neben **Upload a .pem private key and signed certificate** auf **Browse**.

   D. Navigieren Sie zu der Datei mit dem kombinierten privaten Schlüssel und dem signierten PEM-Zertifikat, markieren Sie diese Datei und klicken Sie auf **Öffnen**.

   Wiederholen Sie Schritt 4 für alle Access Gateway-Geräte hinter dem Load Balancer und laden Sie jeweils den privaten Schlüssel und das PEM-Zertifikat auf die einzelnen Access Gateway-Geräte hoch.

Festlegen eines Load Balancers als Standardgateway

Bei einigen Load Balancern oder Netzwerkkonfigurationen muss der Load Balancer als Standardgateway für das Access Gateway festgelegt werden. Wenn Sie den Load Balancer als Standardgateway festlegen, konfigurieren Sie statische Routen auf dem Access Gateway, sodass der gesamte Datenverkehr, der für das sichere Netzwerk bestimmt ist, an ein internes Netzwerk weitergeleitet wird, das diesen internen Datenverkehr problemlos bewältigen kann.

Erhält das Access Gateway ein Paket, das an eine unbekannte IP-Adresse gerichtet ist, wird dieses Paket an die Adresse des Standardgateways übermittelt. Wenn der Load Balancer als Standardgateway konfiguriert ist, sorgt das Access Gateway mit statischem Routing dafür, dass die für die internen Ziele bestimmten Pakete tatsächlich ausgeliefert werden.

Falls das Access Gateway ein Paket empfängt, das für eine interne Adresse bestimmt ist, ohne dass die statische Routingtabelle eine geeignete Route für das Paket aufweist, geht das Paket unter Umständen verloren.

Beispiel: Der Load Balancer ist als Standardgateway konfiguriert und es gilt Folgendes:

- Sie verwenden drei interne Netzwerke: 10.10.0.0, 10.20.0.0 und 10.30.0.0.
- Das Netzwerk 10.10.0.0 kann Pakete an die Netzwerke 10.20.0.0 und 10.30.0.0 weiterleiten. Aber die Netzwerke 10.20.0.0 und 10.30.0.0 können keine Pakete an andere Netzwerke weiterleiten.

In dieser Umgebung müssen auf dem Access Gateway statische Routen für Interface 1 erstellt werden. Diese statischen Routen müssen den gesamten Datenverkehr, der für die Netzwerke 10.20.0.0 und 10.30.0.0 bestimmt ist, über Interface 1 am Access Gateway an das Netzwerk 10.10.0.0 weiterleiten.

Weitere Informationen hierzu finden Sie unter "Konfigurieren von dynamischen und statischen Routen" auf Seite 60.

Konfigurieren des Load Balancing mit Advanced Access Control

Wenn Advanced Access Control gewählt wurde, wird mit dieser Option das Load Balancing für Anmeldeanfragen aktiviert bzw. deaktiviert. Das Kontrollkästchen ist standardmäßig aktiviert, wenn auf zwei Servern Advanced Access Control ausgeführt wird. Das Load Balancing wird nach dem Round-Robin-Prinzip durchgeführt, wobei das System eingehende Anfragen reihum an die Server verteilt, unabhängig von der Serverlast. Wenn es nur einen Server mit Advanced Access Control gibt, ist das Kontrollkästchen nicht verfügbar.

So konfigurieren Sie das Load Balancing mit Advanced Access Control

1. Erweitern Sie im Administration Tool auf der Registerkarte **Access Gateway Cluster** das Fenster für das Access Gateway und klicken Sie auf **Advanced Options**.
2. Klicken Sie auf **Load Balance initial Logon requests** und dann auf **Submit**.

Hinweis: Das Access Gateway-Gerät muss für die Access Gateway Advanced Edition konfiguriert werden, um die Einstellung zu aktivieren.

Konfigurieren von Access Gateway-Failover

Um hohe Verfügbarkeit des internen Netzwerks für Remotebenutzer zu gewährleisten, können Sie zwei oder mehrere Access Gateway-Geräte bereitstellen und für gegenseitiges Failover konfigurieren. In dieser Bereitstellung steht stets ein alternatives Access Gateway zur Verfügung, wenn ein Access Gateway ausfällt. Da das Access Gateway-Failover aktiv/aktiv ist, kann jedes Access Gateway als primäres Gateway für eine andere Gruppe von Benutzern verwendet werden.

Erstes Access Gateway schlägt fehl. Access Gateway Plug-in muss daher zweites Gerät prüfen.
Access Gateway ist nicht verfügbar
Dateiserver
FIREWALL
FIREWALL
Internet
E-Mail-Server
Clientcomputer verwendet Access Gateway Plug-in für Verbindung
Verbindung geht an das zweite Access Gateway
Web- oder Anwendungsserver

Mehrere Access Gateway-Geräte sorgen für Failover

Wenn ein Access Gateway für Failover konfiguriert ist, liefert das Access Gateway eine Failoverliste an das Access Gateway Plug-in.

Während der Erstverbindung vom Access Gateway Plug-in stellt das Access Gateway dem Clientgerät die Failoverliste bereit. Sobald das Clientgerät die Verbindung zum primären Access Gateway verliert, wird die Liste der Failovergeräte durchgegangen. Wenn das primäre Access Gateway ausfällt, versucht das Clientgerät 20 Sekunden lang, die Verbindung wiederherzustellen. Wenn diese Versuche fehlschlagen, wird die Verbindung anhand der Angaben in der Failoverliste hergestellt. Das Clientgerät führt eine DNS-Suche nach dem ersten Failovergerät durch und versucht, eine Verbindung mit diesem Gerät herzustellen. Wenn das erste Failover-Access Gateway nicht verfügbar ist, versucht es das Clientgerät mit dem nächsten Failovergerät. Gelingt es dem Clientgerät, eine Verbindung zu einem Failover-Access Gateway herzustellen, wird das Clientgerät aufgefordert, sich anzumelden.

Sie können bis zu drei Access Gateway-Geräte in die Failoverliste eintragen.

So konfigurieren Sie Failover

1. Klicken Sie auf die Registerkarte **Access Gateway Cluster** und anschließend auf die Registerkarte **Failover Servers**.
2. Geben Sie in den Feldern **First failover appliance**, **Second failover appliance** und/oder **Third failover appliance** die externen IP-Adressen oder die vollqualifizierten Domänennamen der Access Gateways ein, die für Failover verwendet werden sollen.

   Die Access Gateway-Geräte werden in der Reihenfolge für das Failover herangezogen, in der sie in der Liste aufgeführt sind.
3. Geben Sie im Feld **Port** die Portnummer ein. Standardwert ist 443. Klicken Sie auf **Submit**.

Hinweis: In diesem Fall müssen Sie jeweils ein anderes SSL-Serverzertifikat auf den einzelnen Access Gateway-Geräten installieren. Sie können die SSL-Zertifikatsanforderung für die Access Gateway-Failovergeräte mit der Funktion "Certificate Signing Request" im Administration Tool erstellen. Weitere Informationen hierzu finden Sie unter "Erstellen und Installieren von Zertifikaten" auf Seite 51.

Überwachen des Access Gateways

Das Administration Tool ermöglicht den Zugriff auf die Access Gateway-Überwachungstools. Tools, die in früheren Versionen im Administration Desktop des Access Gateways waren, sind jetzt in das Administration Tool integriert.

Sie können die Netzwerkaktivität auf dem Access Gateway auf der Registerkarte **Logging** auf der Registerkarte **Access Gateway Cluster** sehen.

Anwendungsstatistiken finden Sie auf der Registerkarte **Access Gateway Cluster**. Folgende Aufgaben lassen sich auf der Registerkarte **Statistics** durchführen:

- Anzeigen der Access Gateway-Systeminformationen.
- Anzeigen von globalen Statistiken, die aus einer Reihe von Leistungsindikatoren bestehen, die Parameter wie Benutzeranmeldungen und Lizenzverwendung aufzeichnen. Diese Indikatoren werden beim jedem Neustart des Access Gateways zurückgesetzt.
- Anzeigen der aktuellen Benutzer, die mit dem Access Gateway Plug-in, Citrix XenApp Plug-ins oder Citrix Desktop Receiver angemeldet sind.

Auf der Registerkarte **Net Tools** können Sie mehrere Integritätsprüfungen für Access Gateway und das Netzwerk durchführen. Dazu gehören Ping, Traceroute, Portscannen und Packetcapturing.

Dieses Kapitel enthält:

- "Anzeigen und Herunterladen von Systemmeldungsprotokollen"
- "SNMP-Protokolle"
- "Anzeigen von Systemstatistiken"
- "Überwachen der Access Gateway-Operationen"

Anzeigen und Herunterladen von Systemmeldungsprotokollen

Für das Access Gateway gibt es zwei Arten der Protokollierung. Sämtliche Protokolle werden lokal gespeichert und können im Administration Tool oder im Administration Portal angezeigt werden. Bei Bedarf können diese Informationen auch an einen Syslogserver gesendet werden.

Systemmeldungsprotokolle enthalten Informationen, die den Access Gateway-Supportmitarbeitern die Fehlersuche erleichtern können. Durch Prüfung der bereitgestellten Informationen können Sie Änderungen verfolgen, die sich u. U. negativ auf die Stabilität und Leistung des Access Gateways auswirken.

Systemmeldungsprotokolle werden auf dem Access Gateway für die Dauer von 30 Tagen archiviert. Das älteste Protokoll wird dann jeweils durch das aktuelle Protokoll ersetzt. Verwenden Sie einen Syslogserver, um Protokolldateien länger aufzuheben.

Sie können jederzeit einzelne oder auch alle Protokolle herunterladen. Sie können Systemmeldungen auch an Ihren Syslogserver weiterleiten. Informationen hierzu finden Sie unter "Weiterleiten von Systemmeldungen an einen Syslogserver" auf Seite 218.

Hinweis: Wenn Sie über das Administration Tool keine Verbindung zum Access Gateway herstellen können, gehen Sie zum Administration Portal und klicken Sie auf die Registerkarte **Logging**.

So können Sie das Systemprotokoll anzeigen und filtern

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Access Gateway.
2. Klicken Sie auf die Registerkarte **Logging/Settings**.
3. Klicken Sie auf **Show Log File**.

   Das Protokoll für das aktuelle Datum wird angezeigt.

   Wenn Sie das Protokoll für ein früheres Datum anzeigen möchten, wählen Sie in der Liste **Log archive** das entsprechende Datum aus und klicken Sie dann auf **View Log**.

4. So laden Sie ein Protokoll herunter

   - Wählen Sie in der Liste **Log Archive** ein Protokoll aus und klicken Sie neben **Selected Log File** auf Download. Der Protokolldateiname hat standardmäßig folgendes Format: *JJJJMMTT*.log.
   - Wenn Sie alle Protokolle herunterladen möchten, klicken Sie neben **All Log Files** auf **Download**.Der Dateiname ist dann standardmäßig wie folgt: log_archive_*JJJJMMTT*.tgz. Zum Herunterladen von Protokollen vom Access Gateway muss auf Ihrem Computer ein Datenkomprimierungsprogramm, z. B. WinZip, installiert sein. Die Protokolle werden als TGZ-Datei heruntergeladen und müssen dann extrahiert werden. Nach dem Herunterladen einer Datei können Sie deren Inhalt extrahieren und so auf die einzelnen Protokolldateien zugreifen.

Anzeigen der Access Gateway Plug-in-Verbindungsprotokolle

Das Access Gateway-Verbindungsprotokoll enthält Echtzeitinformationen zu Verbindungen, die besonders nützlich beim Beheben von Access Gateway Plug-in-Verbindungsproblemen sind. Sie können über das Access Gateway-Symbol vom Clientgerät auf das Verbindungsprotokoll zugreifen. Der Benutzer kann Ihnen diese Informationen für die Fehlersuche bei Verbindungsproblemen schicken.

So zeigen Sie das Verbindungsprotokoll an

1. Klicken Sie mit der rechten Maustaste im Infobereich der Taskleiste auf das Secure Access-Symbol.
2. Wählen Sie im Kontextmenü den Befehl **Verbindungsprotokoll**.

   Das Verbindungsprotokoll für die Sitzung wird geöffnet.

Hinweis: Das Verbindungsprotokoll wird auf dem Computer des Benutzers unter *%Temp%*\cag_plugin_connection_log.txt gespeichert. Das Protokoll wird bei jedem Einrichten einer neuen Access Gateway-Verbindung überschrieben.

Citrix empfiehlt, die Benutzer aufzufordern, das Verbindungsprotokoll im ausführlichen Modus zu erstellen, da auf diese Weise detaillierte Informationen für die Problembehandlung, z. B. die Zertifikatsüberprüfung, zur Verfügung stehen.

So legen Sie ausführlichen Modus für das Clientverbindungsprotokoll fest

1. Klicken Sie mit der rechten Maustaste auf das Access Gateway-Symbol und klicken Sie dann auf **Verbindungsprotokoll**.
2. Aktivieren Sie im Menü **Optionen** die Option **Ausführlicher Modus**.

Weiterleiten von Systemmeldungen an einen Syslogserver

Das Access Gateway archiviert Systemmeldungen. Informationen hierzu finden Sie unter "Anzeigen und Herunterladen von Systemmeldungsprotokollen" auf Seite 216. Sie können das Access Gateway aber auch anweisen, Systemmeldungen an einen Syslogserver weiterzuleiten.

So leiten Sie Access Gateway-Systemmeldungen an einen Syslogserver weiter

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Access Gateway.
2. Klicken Sie auf die Registerkarte **Logging/Settings**.
3. Geben Sie unter **Syslog Settings** im Feld **Server** die IP-Adresse des Syslogservers ein.
4. Wählen Sie im Feld **Facility** die gewünschte Systemprotokollstufe aus.
5. Geben Sie in das Feld **Broadcast interval (minutes)** eine Sendefrequenz in Minuten ein. Wenn Sie hier 0 eingeben, erfolgt die Protokollierung fortlaufend.
6. Klicken Sie auf **Submit**.

SNMP-Protokolle

Wenn SNMP (Simple Network Management Protocol) aktiviert ist, meldet das Access Gateway die MIB-II-Systemgruppe (1.3.6.1.2.1). Das Access Gateway unterstützt keine Access Gateway-spezifischen SNMP-Daten.

Sie können ein SNMP-Überwachungstool, z. B. Multi Router Traffic Grapher, konfigurieren, um vom Access Gateway gemeldete SNMP-Daten grafisch darzustellen. Ein Beispiel für eine MRTG-Ausgabe finden Sie unter "Beispiel für eine MRTG-Ausgabe" auf Seite 219.

So aktivieren Sie die Protokollierung von SNMP-Meldungen

1. Klicken Sie auf die Registerkarte **Access Gateway Cluster** und anschließend auf die Registerkarte **Logging/Settings**.
2. Wählen Sie unter **SNMP settings** die Option **Enable SNMP**.
3. Geben Sie unter **Location** den SNMP-Speicherort ein. Dieses Feld dient nur zur Information.
4. Geben Sie unter **Contact** den Kontakt ein. Dieses Feld dient nur zur Information.
5. Geben Sie unter **Community** die Community ein. Dieses Feld dient nur zur Information.
6. Geben Sie unter **Port** die Portnummer an.
7. Klicken Sie auf **Submit**.

Beispiel für eine MRTG-Ausgabe

Multi Router Traffic Grapher (MRTG) ist ein Tool zur Überwachung von SNMP-Daten (Verkehrslast usw.). MRTG generiert HTML-Seiten mit PNG-Bildern zur visuellen Darstellung des Verkehrs. Das Tool funktioniert unter UNIX, Windows 2000 Server und Windows Server 2003.

Hinweis: Die Informationen in diesem Abschnitt geben einen allgemeinen Überblick über das Arbeiten mit MRTG. Informationen wie Sie dieses Tool bekommen und verwenden, finden Sie auf der Website von Multi Router Traffic Grapher: http://people.ee.ethz.ch/~oetiker/webtools/mrtg/.

So erfassen Sie SNMP-Daten für das Access Gateway über MRTG (in UNIX)

1. Konfigurieren Sie das Access Gateway für das Antworten auf SNMP-Abfragen. Informationen hierzu finden Sie unter "So aktivieren Sie die Protokollierung von SNMP-Meldungen" auf Seite 219.
2. Erstellen Sie die MRTG-Konfigurationsdateien in /etc/mrtg.

   Die Konfigurationsdateien enthalten Angaben dazu, welche Objekt-IDs vom MRTG-Daemon überwacht werden sollen, von welchem Ziel die SNMP-Daten bezogen werden sollen und wie die MRTG-Ausgabe aussehen soll.

```
WorkDir: /var/www/html/mrtg
Options[_]: nopercent,gauge,noinfo,growright

Target[vpn.myorg.com.tcpCurrEstab]: .1.3.6.1.2.1.6.9.0&.1.3.6.1.2.1.6.9.0:mypswd@10.10.0.30
Xsize[vpn.myorg.com.tcpCurrEstab]: 600
Ysize[vpn.myorg.com.tcpCurrEstab]: 200
Ytics[vpn.myorg.com.tcpCurrEstab]: 10
Title[vpn.myorg.com.tcpCurrEstab]: ESTABLISHED TCP connections
PageTop[vpn.myorg.com.tcpCurrEstab]: <h1>ESTABLISHED TCP connections</h1>
MaxBytes[vpn.myorg.com.tcpCurrEstab]: 1000000
YLegend[vpn.myorg.com.tcpCurrEstab]: # est. conns
ShortLegend[vpn.myorg.com.tcpCurrEstab]:  
LegendI[vpn.myorg.com.tcpCurrEstab]:  Connections: 
LegendO[vpn.myorg.com.tcpCurrEstab]:
Legend1[vpn.myorg.com.tcpCurrEstab]: Established TCP connections
```

MRTG-Konfigurationsdatei

3. Bearbeiten Sie /etc/crontab so, dass alle 5 Minuten eine SNMP-Abfrage durchgeführt wird, anhand derer eine grafische Ausgabe erstellt werden kann. Die einzelnen aufgeführten CFG-Dateien generieren eine separate Ausgabe.
4. Zeigen Sie die Ausgabe in einem Webbrowser an.

   Das Tool speichert die HTML-Ausgabe in dem in der Konfigurationsdatei angegebenen Arbeitsverzeichnis. Der Dateiname der Ausgabe, der mit dem der in Schritt 2 erstellten Konfigurationsdatei übereinstimmt, ist vpn.myorg.com.tcpcurrestab.html.

Anzeigen von Systemstatistiken

Allgemeine Systemstatistiken erhalten Sie, indem Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Access Gateway erweitern und dann auf die Registerkarte **Statistics** klicken.

Es gibt drei Registerkarten mit System-, globalen und Benutzerstatistiken.

Die statistischen Angaben bieten einen Überblick über das Access Gateway und enthalten folgende Informationen:

- Die Version des Access Gateways.
- Dauer der Ausführung des Access Gateways.
- Speichernutzung.
- Maximale und verwendete Verbindungen: Die Angabe der maximalen Verbindungen steht für die Anzahl der Lizenzen, die für die Verwendung mit dem Access Gateway verfügbar sind.
- Anmeldeinformationen für Administratoren, Access Gateway Plug-in- und ICA-Verbindungen.
- Aktuell angemeldete Benutzer.
- Lizenzinformationen für das Access Gateway-Gerät, dass Sie anzeigen.

Überwachen der Access Gateway-Operationen

Das Access Gateway enthält eine Reihe Überwachungsanwendungen, sodass Sie bequem von einem zentralen Standort aus auf die Anwendungen zugreifen können. Die Überwachungsanwendungen sind im dem Administration Tool. Wenn Sie die Registerkarte **Net Tools** auf der Registerkarte **Access Gateway Cluster** wählen, können Sie Netzwerkverbindungen überwachen.

So öffnen Sie die Netzwerküberwachung

Öffnen Sie im Access Gateway Administration Tool auf der Registerkarte **Access Gateway Cluster** das Access Gateway-Fenster und klicken Sie auf die Registerkarte **Net Tools**.

Auf der Registerkarte **Net Tools** können Sie folgende Funktionen verwenden:

- **Ping**: Testen der Verfügbarkeit von Web- und IP-Adressen.
- **Traceroute:** Kombiniert die Funktionalität der Befehle "traceroute" und "ping" in einem Netzwerkdiagnosetool. Wenn Traceroute gestartet wird, untersucht das Tool die Netzwerkverbindung zwischen dem Access Gateway und dem von Ihnen festgelegten Zielhost. Nachdem das Tool die Adresse der einzelnen Netzwerkhops zwischen den Geräten bestimmt hat, sendet es eine ICMP ECHO-Sequenzanforderung an alle, um die Qualität der einzelnen Verbindungen zu den Geräten festzustellen. Dabei druckt es fortlaufende Statistiken zu den einzelnen Geräten.
- **Port Scan:** Zum Ermitteln der DNS-Server im Netzwerk und der geöffneten Ports.
- **Packet Capture:** Interaktives Abfangen von Paketdaten aus einem aktiven Netzwerk oder aus einer zuvor gespeicherten Erfassungsdatei.

Wenn Sie Netzwerküberwachungstools auf einem Clientgerät verwenden, können Sie möglicherweise eingehende TCP-Verbindungen auf verschiedenen hohen Portnummern beobachten. Diese Verbindungen finden nicht wirklich statt. Sie werden von der NDIS shim-Komponente initiiert.

Aus diesem Grund müssen IP-Firewall-Regeln auf dem Clientgerät so konfiguriert sein, dass Datenverkehr vom und zum Access Gateway sowie zu Ziel-IP-Adressen erlaubt ist. Lokal, also auf dem Clientgerät, wird der gesamte verbindungsspezifische Verkehr (wie SYN-ACK-, PUSH-, ACK- und FIN-Pakete) vom Access Gateway Plug-in neu erstellt, damit es so aussieht, als käme er vom privaten Server. Der Client sendet physischen Datenverkehr nur über Port 443 an das Gateway.

Bei der Clientinitialisierung sind fünf UDP-Socketverbindungen sichtbar. Dies sind:

- 10000 UDP steuert die Informationen zwischen dem Netzwerktreiber und der Portweiterleitung.
- 10010 TCP/UPD ist die Datennutzlast.
- 10020 UDP wird für DNS verwendet.
- 10030 UDP wird für ICMP verwendet.
- 10040 UDP ist für zukünftige Verwendung reserviert.

Sichern von Verbindungen mit digitalen Zertifikaten

Dieses Kapitel enthält eine Übersicht der in der Access Gateway-Lösung verwendeten Sicherheitstechnologien und soll Ihnen helfen, Anzahl und Typ der jeweils erforderlichen Zertifikate zu ermitteln und zu entscheiden, wie und wo Sie diese erhalten und installieren.

Dieses Kapitel enthält:

- "Einführung in Sicherheitsprotokolle, Kryptografie und digitale Zertifikate"
- "Beantragen von Zertifikaten"
- "Beantragen von Serverzertifikaten"
- "Verwenden von Windows-Zertifikaten"
- "Anfordern von Zertifikaten für interne Verbindungen"
- "Verwenden von Platzhalterzertifikaten"

Wichtig: Verwenden Sie zum Konfigurieren von Zertifikaten keine 512-Bit-Schlüsselpaare, da diese oft Opfer von Brute-Force-Angriffen werden.

Einführung in Sicherheitsprotokolle, Kryptografie und digitale Zertifikate

Dieser Abschnitt enthält eine Einführung in das SSL (Secure Sockets Layer)- und das TSL (Transport Layer Security)-Protokoll und bietet einen Überblick über Kryptografie und die Public Key Infrastructure (PKI).

Einführung in Sicherheitsprotokolle

SSL und TLS sind führende Internetprotokolle, die Sicherheit für E-Commerce, Webdienste und viele andere Netzwerkfunktionen bieten.

Das SSL-Protokoll ist der aktuelle Standard für den sicheren Informationsaustausch im Internet. Dieses ursprünglich von Netscape entwickelte Protokoll wurde enorm wichtig für den Internetbetrieb. Daher übernahm die IETF (Internet Engineering Taskforce) die Aufgabe, SSL als offenen Standard zu entwickeln. Um SSL von anderen Entwicklungsarbeiten zu unterscheiden, wurde SSL von der IETF in TLS umbenannt. Das TLS-Protokoll stammt von der dritten SSL-Version ab, wobei TLS1.0 SSL3.1 entspricht.

Einige Organisationen, u. a. amerikanische Regierungsstellen, verlangen das Sichern der Datenkommunikation mit TLS. Diese Organisationen verlangen u. U. auch die Verwendung verifizierter Kryptografie.

Mit dem SSL/TLS-Protokoll können sicherheitskritische Daten über öffentliche Netzwerke, wie das Internet, übertragen werden. Dieses Protokoll bietet die folgenden wichtigen Sicherheitsfunktionen:

- **Authentifizierung:** Ein Client kann die Identität eines Servers ermitteln und feststellen, dass der Server kein Betrüger ist. Optional kann ein Server auch die Identität des Clients authentifizieren, der Verbindungen anfordert.
- **Datenschutz:** Die zwischen dem Client und dem Server übertragenen Daten werden verschlüsselt, damit sie nicht entschlüsselt werden können, falls Nachrichten von Dritten abgefangen werden.
- **Datenintegrität:** Der Empfänger verschlüsselter Daten weiß, ob diese von einem Dritten manipuliert oder geändert wurden.

Einführung in die Kryptografie

Für die sichere Datenübertragung nutzt das SSL/TLS-Protokoll *Kryptografie*. Mit Kryptografie können Nachrichten verschlüsselt werden, um die Vertraulichkeit zu gewährleisten. Kryptografie dient auch zur Authentifizierung der Identität einer Nachrichtenquelle und zur Gewährleistung der Integrität ihres Inhalts.

Nachrichten werden mit einem Geheimcode, einer sogenannten *Verschlüsselungssammlung*, übertragen. Mit der Verschlüsselungssammlung wird eine Nachricht verschlüsselt, damit sie nur vom Absender und Empfänger verstanden werden kann. Da nur der Empfänger, der den Geheimcode hat, die ursprüngliche Nachricht entschlüsseln kann, ist die Vertraulichkeit gewährleistet.

Mit Kryptografie kann der Absender spezielle Informationen in eine Nachricht aufnehmen, die nur dem Absender und Empfänger bekannt sind. Der Empfänger kann die Nachricht durch Prüfen dieser speziellen Informationen authentifizieren.

Durch Kryptografie ist auch gewährleistet, dass der Inhalt einer Nachricht nicht geändert wird. Zu diesem Zweck schließt der Absender einen kryptografischen Vorgang namens *Hashfunktion* in die Nachricht ein. Eine Hashfunktion ist eine mathematische Darstellung der Informationen und lässt sich mit den Prüfsummen in Datenübertragungsprotokollen vergleichen. Bei Eingang der Daten an ihrem Zielort wird die Hashfunktion vom Empfänger berechnet. Wenn der Wert der vom Empfänger berechneten Hashfunktion mit dem des Absenders übereinstimmt, ist die Integrität der Nachricht gewährleistet.

Kryptografietypen

Im Wesentlichen werden zwei Kryptografietypen unterschieden:

- Kryptografie mit einem Geheimschlüssel
- Kryptografie mit einem öffentlichen Schlüssel

In kryptografischen Systemen bezieht sich der Begriff *Schlüssel* auf einen numerischen Wert, der von einem Algorithmus zum Ändern von Informationen verwendet wird, wodurch diese Informationen geschützt und nur für die Personen sichtbar sind, die über den entsprechenden Schlüssel zum Abfragen der Informationen verfügen.

Die **Kryptografie mit einem Geheimschlüssel** wird auch als *symmetrische Verschlüsselung* bezeichnet. Bei diesem Kryptografietyp kennen Absender und Empfänger denselben Geheimcode, den sogenannten *Schlüssel*. Das Verschlüsseln von Nachrichten auf Seiten des Absenders und das Entschlüsseln auf Seiten des Empfängers erfolgt mit demselben Schlüssel.

Dieses Verfahren eignet sich für die Datenübertragung bei einer begrenzten Personenzahl, ist allerdings für den Austausch von Geheimschlüsseln bei einer Vielzahl von Personen impraktikabel. Außerdem ist die sichere Mitteilung des Geheimschlüssels problematisch.

Bei der **Kryptografie mit einem öffentlichen Schlüssel**, der sogenannten *asymmetrischen Verschlüsselung*, wird ein Schlüsselpaar für die Verschlüsselung und Entschlüsselung verwendet. Dieses Kryptografieverfahren basiert auf Schlüsselpaaren, nämlich dem *öffentlichen* und dem *privaten* Schlüssel.

Der öffentliche Schlüssel kann ohne Gefährdung des privaten Schlüssels weitergeleitet werden; letzterer muss von seinem Eigentümer geheim gehalten werden. Da diese Schlüssel nur paarweise funktionieren, lässt sich die mit dem öffentlichen Schlüssel vorgenommene Verschlüsselung nur mit dem entsprechenden privaten Schlüssel entschlüsseln. Das folgende Beispiel veranschaulicht die Arbeitsweise des Kryptografieverfahrens mit einem öffentlichen Schlüssel:

- Frau Meier möchte geheime Informationen mit Herrn Müller austauschen. Frau Meier verschlüsselt ihre Nachricht mit dem öffentlichen Schlüssel von Herrn Müller (den Herr Müller öffentlich bekannt gegeben hat) und leitet die verschlüsselte Nachricht an Herrn Müller weiter.
- Wenn Herr Müller die Nachricht erhält, entschlüsselt er sie mit seinem privaten Schlüssel, damit er die Nachricht lesen kann.
- Wenn Herr Müller eine Antwort an Frau Meier sendet, verschlüsselt er die Nachricht mit dem öffentlichen Schlüssel von Frau Meier.
- Bei Eingang der Antwort von Herrn Müller entschlüsselt Frau Meier seine Nachricht mit ihrem privaten Schlüssel.

Der wesentliche Vorzug der asymmetrischen Verschlüsselung im Vergleich zur symmetrischen Verschlüsselung besteht darin, dass sich Absender und Empfänger keine Schlüssel im Voraus mitteilen müssen. Sofern der private Schlüssel geheim gehalten wird, ermöglichen öffentliche Schlüssel die Weiterleitung vertraulicher Informationen.

Kombinieren der Kryptografieverfahren mit öffentlichen und geheimen Schlüsseln: Der größte Nachteil der Kryptografie mit einem öffentlichen Schlüssel besteht darin, dass die Verschlüsselung mit den in der PKI üblichen, sehr langen Schlüsseln bei den meisten Computersystemen zu Leistungsproblemen führen kann. Aus diesem Grund werden bei der Kryptografie häufig öffentliche und private Schlüssel kombiniert verwendet. Das folgende Beispiel veranschaulicht die Arbeitsweise:

- Herr Müller möchte geheime Informationen mit Frau Meier austauschen und erhält daher ihren öffentlichen Schlüssel. Außerdem erstellt er nur für diese Sitzung eine beliebige Ziffernfolge, auch *Sitzungsschlüssel* genannt.
- Herr Müller verwendet den öffentlichen Schlüssel von Frau Meier zum Chiffrieren des Sitzungsschlüssels.
- Herr Müller leitet die verschlüsselte Nachricht und den chiffrierten Sitzungsschlüssel an Frau Meier weiter.
- Frau Meier verwendet ihren privaten Schlüssel, um die Nachricht von Herrn Müller zu entschlüsseln und den Sitzungsschlüssel zu extrahieren.

Wenn Herr Müller und Frau Meier den Sitzungsschlüssel mit Erfolg austauschen, erübrigt sich die Kryptografie mit einem öffentlichen Schlüssel. Der Daten- und Informationsaustausch erfolgt dann nur auf Basis des Sitzungsschlüssels. Die Verschlüsselung mit einem öffentlichen Schlüssel wird beispielsweise zur Weiterleitung des geheimen Schlüssels verwendet. Beim Austausch des geheimen Schlüssels erfolgt die Datenübertragung durch Verschlüsselung mit dem geheimen Schlüssel.

Diese Lösung bietet die Vorzüge beider Verfahren, d. h. die Geschwindigkeit der Verschlüsselung mit einem geheimen Schlüssel und die Sicherheit der Verschlüsselung mit einem öffentlichen Schlüssel.

Digitale Zertifikate und Zertifizierungsstellen

Wie kann Frau Meier bei den oben beschriebenen Szenarien sicher sein, dass Herr Müller wirklich Herr Müller und kein Betrüger ist? Wenn Frau Meier ihren öffentlichen Schlüssel weiterleitet, muss auch Herr Müller sicher sein, dass Frau Meier tatsächlich die Person ist, die sie zu sein vorgibt.

Das ISO X.509-Protokoll definiert einen Mechanismus, ein sogenanntes *Zertifikat*, das den öffentlichen, von einer vertrauenswürdigen Organisation, einer sogenannten *Zertifizierungsstelle*, signierten Schlüssel eines Benutzers enthält.

Zertifikate enthalten Informationen zum Festlegen von Identitäten in einem Netzwerk bei einem Prozess, der *Authentifizierung* genannt wird. Wie Führerscheine, Pässe oder sonstige Identitätsnachweise ermöglichen Zertifikate die gegenseitige Authentifizierung von Servern und Clients, bevor eine sichere Verbindung hergestellt wird.

Zertifikate sind nur für die Dauer eines bestimmten Zeitraums gültig. Bei Ablauf der Gültigkeitsdauer muss ein neues Zertifikat ausgestellt werden. Die Zertifizierungsstelle kann Zertifikate auch sperren.

Zur Herstellung einer SSL/TLS-Verbindung ist an einem Ende der Verbindung ein Serverzertifikat und am anderen Ende der Verbindung ein Stammzertifikat der Zertifizierungsstelle erforderlich, die das Serverzertifikat ausgestellt hat.

- **Serverzertifikat:** Mit einem Serverzertifikat wird die Identität eines Servers bestätigt. Das für das Access Gateway erforderliche digitale Zertifikat wird *Serverzertifikat* genannt.
- **Stammzertifikat:** Ein Stammzertifikat dient zur Identifizierung der Zertifizierungsstelle, die das Serverzertifikat signiert hat. Das Stammzertifikat gehört der Zertifizierungsstelle. Anhand dieses digitalen Zertifikats überprüft ein Clientgerät das Serverzertifikat.

Beim Herstellen einer SSL-Verbindung mit einem Webbrowser auf einem Clientgerät leitet der Server sein Zertifikat an das Clientgerät weiter.

Bei Eingang eines Serverzertifikats prüft der Webbrowser (z. B. Internet Explorer) auf dem Clientgerät, welche Zertifizierungsstelle das Zertifikat ausgestellt hat und ob diese Zertifizierungsstelle für den Client vertrauenswürdig ist. Wenn die Zertifizierungsstelle nicht vertrauenswürdig ist, fordert der Webbrowser den Benutzer auf, das Zertifikat zu akzeptieren oder abzulehnen (d. h. den Zugriff auf diese Website zu akzeptieren oder abzulehnen).

Wenn Frau Meier jetzt eine Nachricht von Herrn Müller erhält, wird anhand der lokal gespeicherten Informationen über die Zertifizierungsstelle geprüft, ob diese Zertifizierungsstelle das Zertifikat auch tatsächlich ausgestellt hat. Diese Informationen sind eine Kopie des eigenen Zertifikats der Zertifizierungsstelle und werden als *Stammzertifikat* bezeichnet.

In der Regel haben Zertifikate ein gemeinsames Format, das normalerweise auf ITU-Standards basiert. Zertifikate enthalten u. a. folgende Informationen:

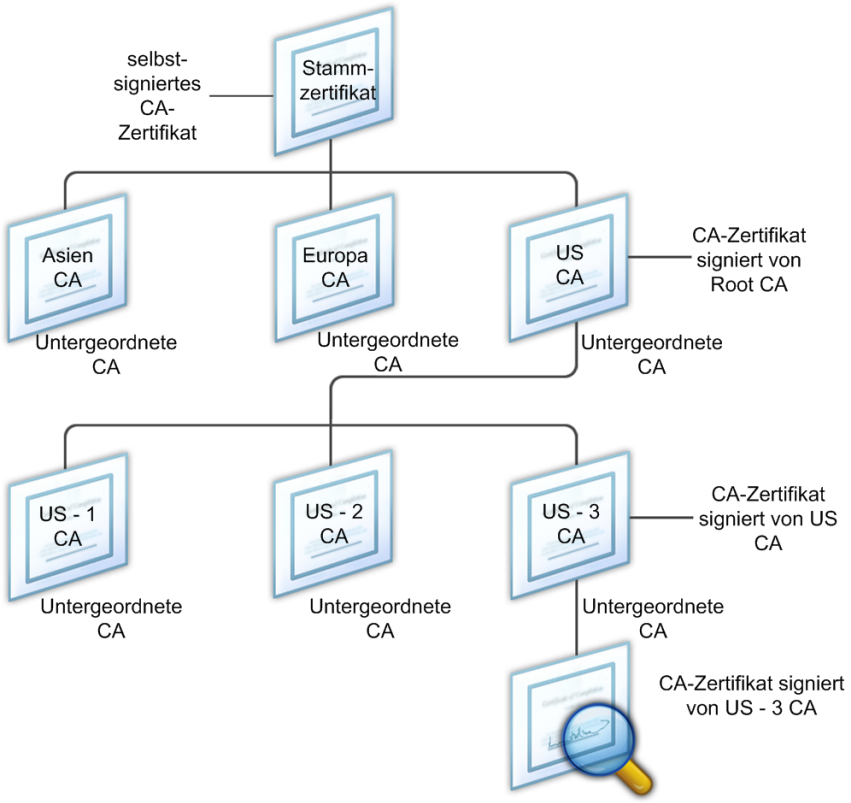
- **Aussteller:** Die Organisation, von der die Zertifikate ausgestellt werden.
- **Betreff:** Die Identität, die durch das Zertifikat identifiziert wird.
- **Gültigkeitsdauer:** Das Start- und Ablaufdatum eines Zertifikats.
- **Öffentlicher Schlüssel:** Der zum Verschlüsseln der Daten verwendete öffentliche Schlüssel des Betreffs.
- Signatur des Ausstellers: Die digitale Signatur der Zertifizierungsstelle für das Zertifikat, anhand dessen seine Authentizität gewährleistet wird.

Einige Unternehmen und Organisationen fungieren derzeit als Zertifizierungsstellen, u. a. VeriSign, Baltimore, Entrust und ihre jeweiligen verbundenen Unternehmen.

Zertifikatketten

Einige Organisationen delegieren die Ausstellung von Zertifikaten, um das mit der räumlichen Trennung zwischen Organisationseinheiten einhergehende Problem oder das Problem, das auf die Anwendung unterschiedlicher Ausstellungsrichtlinien für verschiedene Organisationsbereiche zurückzuführen ist, zu lösen.

Die Verantwortung für die Ausstellung von Zertifikaten kann durch die Einrichtung von untergeordneten Zertifizierungsstellen delegiert werden. Der X.509-Standard enthält ein Modell, mit dem sich eine Hierarchie von Zertifizierungsstellen einrichten lässt. Bei diesem Modell ist die Stammzertifizierungsstelle auf der obersten Hierarchieebene und hat ein selbstsigniertes Zertifikat. Die der Stammzertifizierungsstelle direkt untergeordneten Zertifizierungsstellen lassen Zertifizierungsstellenzertifikate von der Stammzertifizierungsstelle signieren. Zertifizierungsstellen, die in der Hierarchie unter den untergeordneten Zertifizierungsstellen sind, lassen ihre Zertifizierungsstellenzertifikate von den untergeordneten Zertifizierungsstellen signieren.



Hierarchische Struktur einer typischen digitalen Zertifikatkette

Zertifizierungsstellen können ihre eigenen Zertifikate signieren (d. h. sie sind selbst signiert) oder sie können auch von einer anderen Zertifizierungsstelle signiert werden. Selbst signierte Zertifikate stammen von sogenannten *Stammzertifizierungsstellen*. Nicht selbst signierte Zertifikate stammen von sogenannten *untergeordneten Zertifizierungsstellen* oder *Zwischenzertifizierungsstellen.*

Wenn ein Zertifikat von einer Zertifizierungsstelle mit einem selbstsignierten Zertifikat signiert ist, setzt sich die Zertifikatkette aus genau zwei Zertifikaten zusammen: dem Zertifikat der Endeinheit und dem Zertifikat der Stammzertifizierungsstelle. Wenn ein Benutzer- oder Serverzertifikat von einer Zwischenzertifizierungsstelle signiert ist, ist die Zertifikatkette länger.

Die nachstehende Abbildung zeigt, dass die ersten beiden Elemente das Endeinheitszertifikat (in diesem Fall gwy01.firma.com) und das Zertifikat der Zwischenzertifizierungsstelle, und zwar in dieser Reihenfolge, sind. Nach dem Zertifikat der Zwischenzertifizierungsstelle folgt das Zertifikat ihrer Zertifizierungsstelle. Das letztgenannte Zertifikat in dieser Liste ist das Zertifikat der Stammzertifizierungsstelle. Jedes Zertifikat in der Kette bestätigt die Identität des vorhergehenden Zertifikats.

Typische Kette digitaler Zertifikate

Zertifikatsperrlisten

Gelegentlich veröffentlichen Zertifizierungsstellen Zertifikatsperrlisten. Zertifikatsperrlisten enthalten Informationen über nicht mehr vertrauenswürdige Zertifikate. Beispiel: Frau Meier verlässt das Unternehmen XYZ. Das Unternehmen kann das Zertifikat von Frau Meier auf eine Zertifikatsperrliste setzen, damit sie keine Nachrichten mehr mit diesem Schlüssel signieren kann.

Auf ähnliche Weise können Sie ein Zertifikat sperren, wenn ein privater Schlüssel öffentlich bekannt geworden ist oder wenn dieses Zertifikat abgelaufen und ein neues Zertifikat gültig ist. Bevor Sie einem öffentlichen Schlüssel trauen, sollten Sie sich vergewissern, dass das Zertifikat in keiner Zertifikatsperrliste aufgeführt ist.

Ablaufen und Erneuern von Zertifikaten

Zertifikate werden mit einer geplanten Lebensdauer (Gültigkeitsdauer) und einem ausdrücklichen Ablaufdatum ausgestellt. Nach dem Ausstellen werden Zertifikate bis zum Erreichen ihres Ablaufdatums als gültig angesehen. Nach dem Ablaufdatum kann ein Zertifikat nicht mehr zum Validieren einer Benutzersitzung verwendet werden. Diese Richtlinie dient zur Erhöhung der Sicherheit, da das Gefährdungspotenzial solcher Zertifikate eingeschränkt wird. Diese Ablaufdaten werden von der ausstellenden Zertifizierungsstelle festgelegt.

Normalerweise müssen Sie ein Zertifikat vor Erreichen seines Ablaufdatums erneuern. Die meisten Zertifizierungsstellen bieten einen gut dokumentierten Prozess für das Erneuern von Zertifikaten. Auf der Website Ihrer Zertifizierungsstelle finden Sie detaillierte Anweisungen zum Erneuern von Zertifikaten.

Beantragen von Zertifikaten

Beim Ermitteln der für Ihre Access Gateway-Bereitstellung erforderlichen Anzahl und Art von Zertifikaten müssen Sie entscheiden, bei welcher Stelle die Zertifikate zu beantragen sind. Diese Entscheidung hängt von mehreren Faktoren ab, wie u. a.:

- Ob Ihre Organisation eine Zertifizierungsstelle ist. Dies ist vermutlich nur bei sehr großen Unternehmen der Fall.
- Ob Ihre Organisation bereits Geschäftsbeziehungen zu einer öffentlichen Zertifizierungsstelle hat.
- Das Windows-Betriebssystem unterstützt mehrere öffentliche Zertifizierungsstellen.
- Zertifikatkosten, Ruf einer bestimmten öffentlichen Zertifizierungsstelle usw.

Ihre Organisation hat eine eigene Zertifizierungsstelle

Wenn Ihre Organisation eine eigene Zertifizierungsstelle hat, müssen Sie entscheiden, ob die organisationseigenen Zertifikate für die Sicherung der Datenübertragung in der Access Gateway-Umgebung verwendet werden sollen. Citrix empfiehlt, dass Sie sich mit Ihrer organisationseigenen Sicherheitsabteilung in Verbindung setzen, um diese Frage zu klären und nähere Anweisungen zu erhalten, wie Sie Zertifikate erhalten.

Wenn Sie nicht sicher sind, ob Ihre Organisation über eine eigene Zertifizierungsstelle verfügt, sollten Sie sich mit der Sicherheitsabteilung oder dem Sicherheitsexperten Ihrer Organisation in Verbindung setzen.

Ihre Organisation hat keine eigene Zertifizierungsstelle

Wenn Ihre Organisation keine eigene Zertifizierungsstelle hat, müssen Sie Ihre Zertifikate bei einer öffentlichen Zertifizierungsstelle, wie beispielsweise VeriSign, beantragen.

Das Beantragen eines digitalen Zertifikats bei einer öffentlichen Zertifizierungsstelle schließt den folgenden Verifizierungsprozess ein:

- Auf Basis der von Ihrer Organisation vorgelegten Informationen kann die Zertifizierungsstelle die vermeintliche Identität Ihrer Organisation überprüfen. Dabei können andere Organisationsabteilungen in den Verifizierungsprozess eingebunden werden, wie beispielsweise die Buchhaltung. Unter Umständen muss die Gründungsurkunde oder ein ähnliches Rechtsdokument vorgelegt werden.
- Personen mit der entsprechenden Bevollmächtigung in Ihrer Organisation müssen die von der Zertifizierungsstelle vorgelegten rechtsverbindlichen Vereinbarungen unterzeichnen.
- Da die Zertifizierungsstelle Ihre Organisation als Käufer prüft, ist die Einkaufsabteilung bei diesem Prozess vermutlich involviert.
- Sie legen der Zertifizierungsstelle die Kontaktinformationen der jeweiligen Ansprechpartner vor, die bei Fragen angerufen werden können.

Beantragen von Serverzertifikaten

Der Sicherheitsexperte Ihrer Organisation ist wahrscheinlich mit der Beschaffung von Serverzertifikaten vertraut. Auf den Websites gängiger Zertifizierungsstellen, wie beispielsweise von VeriSign, finden Sie Anweisungen zum Erstellen von Serverzertifikaten mit verschiedenen Webserverprodukten. Weitere Informationen zum Erstellen einer Zertifikatsanforderung finden Sie unter "Erstellen und Installieren von Zertifikaten" auf Seite 51.

Hinweis: Mehrere Zertifizierungsstellen bieten Testserverzertifikate für einen befristeten Zeitraum an. Es könnte sinnvoll sein, ein Testzertifikat zum Testen des Access Gateways zu beantragen, bevor es in einer Produktionsumgebung bereitgestellt wird. Dabei sollten Sie darauf achten, dass Sie die entsprechenden Teststammzertifikate herunterladen und auf jedem Clientgerät installieren, das eine Verbindung über das Access Gateway herstellt.

Digitale Zertifikate und deren Verwendung im Access Gateway

Das Access Gateway verwendet digitale Zertifikate zum Verschlüsseln und Authentifizieren von über eine Verbindung gesendetem Verkehr. Wenn das auf dem Access Gateway installierte digitale Zertifikat nicht von einer Zertifizierungsstelle signiert ist, wird der Verkehr zwar verschlüsselt, aber nicht authentifiziert. Die Authentifizierung des Verkehrs erfolgt nur, wenn das digitale Zertifikat von einer Zertifizierungsstelle signiert ist.

Wenn über eine Verbindung gesendeter Verkehr nicht authentifiziert wird, kann es bei der Verbindung zu Man-in-the-Middle-Angriffen kommen. Bei einem solchen Angriff fangen Dritte den öffentlichen Schlüssel ab, der vom Access Gateway an das Access Gateway-Plug-in gesendet wird, und nutzen diesen, um das Access Gateway vorzutäuschen. Die Folge ist, dass der Benutzer, ohne es zu wissen, Authentifizierungsinformationen an den Angreifer sendet, der mit diesen Informationen eine Verbindung zum Access Gateway herstellen kann. Mit Zertifikaten, die von einer Zertifizierungsstelle signiert sind, werden solche Angriffe verhindert.

Wenn das auf dem Access Gateway installierte Zertifikat nicht von einer Zertifizierungsstelle signiert ist, wird Access Gateway Plug-in-Benutzern bei der Anmeldung eine Sicherheitswarnung angezeigt.

Eine solche Sicherheitswarnung wird Access Gateway Plug-in-Benutzern so lange angezeigt, bis Sie ein von einer Zertifizierungsstelle signiertes Zertifikat auf dem Access Gateway und ein entsprechendes Zertifikat auf den Computern der Benutzer installiert haben. Benutzer können die Sicherheitswarnung im Dialogfeld mit den Secure Access-Verbindungseigenschaften auch deaktivieren.

Verwenden von Windows-Zertifikaten

Das Access Gateway enthält den Certificate Request Generator, mit dem automatisch eine Zertifikatsanforderung erstellt werden kann. Nachdem die Datei von der Zertifizierungsstelle zurückgesendet wurde, kann sie auf das Access Gateway hochgeladen werden. Die hochgeladene Datei wird automatisch in das korrekte Format umgewandelt.

Wenn Sie zum Erstellen des signierten Zertifikats nicht den Certificate Request Generator verwenden möchten, empfiehlt Citrix, für die Verwaltung von Zertifikatsaufgaben Win32 OpenSSL zu verwenden. Nähere Informationen zu Win32 Open SSL finden Sie auf der OpenSSL-Website unter http://www.openssl.org/. Binärdateien für Win32 Open SSL können von der Website http://www.openssl.org/related/binaries.html heruntergeladen werden.

Wenn Sie mit der Manipulation von Zertifikaten vertraut sind, können Sie auch Tools verwenden, um eine PEM-formatierte Datei zu erstellen. Das Zertifikat, das Sie auf das Access Gateway hochladen, muss die folgenden Eigenschaften haben:

- Das Zertifikat muss im PEM-Format vorliegen und einen privaten Schlüssel enthalten.
- Das signierte Zertifikat und der private Schlüssel müssen unverschlüsselt sein. Wenn zum Entschlüsseln ein Kennwort vorhanden ist, kann ein verschlüsselter öffentlicher Schlüssel verwendet werden.

Entschlüsseln des privaten Schlüssels

Führen Sie die hier genannten Schritte nur aus, wenn die Methode, die Sie zum Generieren des privaten Schlüssels verwenden, einen verschlüsselten Schlüssel zum Ergebnis hat.

So entschlüsseln Sie den privaten Schlüssel

1. Geben Sie an der $-Eingabeaufforderung den folgenden Befehl ein: **openssl rsa**

   Wenn Sie diesen Befehl ohne Argumente eingeben, erhalten Sie folgende Aufforderung:

   ```
   read RSA key
   ```

2. Geben Sie den Namen des zu entschlüsselnden Kennworts ein.

   Wenn Sie den Namen des privaten Schlüssels und der entschlüsselten PEM-Datei kennen, können Sie auch den Befehl **openssl rsa** mit den zugehörigen Argumenten eingeben.

   Wenn der Dateiname des privaten Schlüssels z. B. **mein_schlüsseltag_schlüssel.pvk** und der entschlüsselte Dateiname **ausgabe_schlüssel.pem** ist, geben Sie Folgendes ein: **openssl rsa -in mein_schlüsseltag_schlüssel.pvk -out ausgabe_schlüssel.pem**.

Weitere Informationen finden Sie auf der Open SSL-Website unter http://www.openssl.org/docs/apps/rsa.html#EXAMPLES.

Weitere Informationen über das Herunterladen von OpenSSL für Windows finden Sie auf der SourceForge-Website unter http://sourceforge.net/project/showfiles.php?group_id=23617&release_id=48801.

Umwandeln in ein PEM-formatiertes Zertifikat

Es ist möglich, dass das signierte Zertifikat, das Sie von der Zertifizierungsstelle erhalten, nicht das PEM-Format hat. Wenn die Datei im Binärformat (DER) vorliegt, wandeln Sie sie wie folgt in ein PEM-Format um:

openssl x509 -in *Zertifikatdatei* **-inform DER -outform PEM -out** *umgewandelteZertifikatdatei*

Verwendet das Zertifikat bereits ein Textformat, könnte es das PKCS-Format sein. Zu PKCS-formatierten Zertifikaten kommt es, wenn Sie angeben, dass das Zertifikat in einem Microsoft- und nicht in einem Apache-Betriebssystem verwendet werden wird. Wenn das Zertifikat nicht im PEM-Format vorliegt, wird bei Eingabe des folgenden Befehls eine Fehlermeldung ausgegeben. *Zertifikatdatei* darf bei der Ausführung dieses Befehls nicht den privaten Schlüssel enthalten.

openssl verify -verbose -CApath /tmp *Zertifikatdatei*

Wenn dieser Befehl zur Ausgabe der folgenden Fehlermeldung führt, hat die Datei nicht das PEM-Format.

```
certFile: unable to load certificate file
4840:error:0906D064:PEM routines:PEM_read_bio:bad
base64decode:pem_lib.c:781:
```

So wandeln Sie das Zertifikat vom PKCS7- in das PEM-Format um

1. Führen Sie den folgenden Befehl aus:

   openssl pkcs7 -in ./*Zertifikatdatei* **-print_certs**

   Das Ergebnis sieht in etwa wie folgt aus:

   ```
   subject=...
   ...
   -----BEGIN CERTIFICATE-----
   ... Server Certificate ...
   -----END CERTIFICATE-----

   subject=...

   ...
   -----BEGIN CERTIFICATE-----
   ... Intermediate Cert ...
   -----END CERTIFICATE-----
   ```

2. Kombinieren Sie die Serverzertifikatsdaten und die Zwischenzertifikatsdaten (sofern vorhanden) der Ausgabe mit dem privaten Schlüssel. Informationen hierzu finden Sie unter "Kombinieren des privaten Schlüssels mit dem signierten Zertifikat" auf Seite 237 und "Generieren vertrauenswürdiger Zertifikate für mehrere Ebenen" auf Seite 238.

Kombinieren des privaten Schlüssels mit dem signierten Zertifikat

Sie müssen das signierte Zertifikat mit dem privaten Schlüssel kombinieren. Erst dann können Sie es auf das Access Gateway hochladen.

So kombinieren Sie den privaten Schlüssel mit dem signierten Zertifikat

1. Verwenden Sie einen Texteditor, um den unverschlüsselten privaten Schlüssel mit dem signierten Zertifikat im PEM-Dateiformat zu kombinieren.

   Der Dateiinhalt muss in etwa wie folgt aussehen:

   ```
   -----BEGIN RSA PRIVATE KEY-----
   <Unverschlüsselter privater Schlüssel>
   -----END RSA Private KEY-----
   -----BEGIN CERTIFICATE-----
   <Signiertes Zertifikat>
   -----END CERTIFICATE-----
   ```

2. Speichern Sie die PEM-Datei und geben Sie ihr dabei einen Namen, wie z. B. **AccessGateway.pem**.

Generieren vertrauenswürdiger Zertifikate für mehrere Ebenen

Sie müssen herausfinden, ob Ihr Zertifikat mehrere Ebenen hat und, falls dies zutrifft, die Zwischenzertifikate entsprechend handhaben.

Achtung: Alle Zertifikate für das Access Gateway, die mehr als eine Ebene haben, *müssen* sämtliche Zwischenzertifikate enthalten, da das System andernfalls unbrauchbar werden könnte.

So generieren Sie vertrauenswürdige Stammzertifikate für mehrere Ebenen

1. Öffnen Sie den Internet Explorer und öffnen Sie über das Access Gateway eine Webadresse. Geben Sie z. B. eine Adresse wie die folgende ein:

   https://*IP-Adresse***:***httpPort***//www.***meineseite***.com**

   wobei gilt:

   IP-Adresse ist die IP-Adresse des Access Gateways.

   httpPort ist die Access Gateway-Portnummer.

2. Doppelklicken Sie auf das Schlosssymbol in der rechten unteren Ecke des Browsers.
3. Wechseln Sie zur Registerkarte "Zertifizierungspfad".
4. Doppelklicken Sie auf die erste Pfadebene, um die Zertifikatsinformationen für die erste Ebene aufzurufen, und klicken Sie auf die Registerkarte **Details**.
5. Klicken Sie unten auf die Schaltfläche **In Datei kopieren**.
6. Klicken Sie auf der ersten Seite des Zertifikatsexport-Assistenten auf **Weiter**.
7. Klicken Sie auf **Base-64-codiert** und anschließend auf **Weiter**.
8. Geben Sie einen Dateinamen an. Beispiel G:\tmp\servercert.cer. Überprüfen Sie die Informationen und notieren Sie sich den vollständigen Dateinamen. Klicken Sie auf **Fertig stellen**.
9. Klicken Sie auf **OK**, um das Fenster **Zertifikat** für die erste Ebene zu schließen.
10. Wiederholen Sie die Schritte 4 bis 10 für alle Ebenen außer der letzten Ebene.

11. Speichern Sie alle Zertifikate in einer Datei und stellen Sie sicher, dass sämtliche Zwischenzertifikate in der Zertifikatdatei enthalten sind, die Sie hochladen.

Die Datei zum Hochladen muss das folgende Format haben:

```
private key
Server Certificate
Intermediate Certificate 0
Intermediate Certificate 1
Intermediate Certificate 2
```

Anfordern von Zertifikaten für interne Verbindungen

Um die Sicherheit interner Verbindungen zu erhöhen, die vom Access Gateway ausgehen, können Sie festlegen, dass das Access Gateway die SSL-Serverzertifikate validieren muss. Das Überprüfen von SSL-Serverzertifikaten ist eine wichtige Sicherheitsmaßnahme, da so Sicherheitsverletzungen wie Man-in-the-Middle-Angriffe zu verhindert werden können.

Diese Einstellung bestimmt, ob SSL-Serverzertifikate für vom Access Gateway zum internen Netzwerk initiierte Verbindungen überprüft werden. Die SSL-Serverzertifikate werden geprüft, die das Webinterface und die Secure Ticket Authority präsentiert.

Durch das Erzwingen der Überprüfung der SSL-Serverzertifikate erhöht sich die Sicherheit bei Verbindungen zwischen dem Access Gateway und den Servern, auf denen Access Gateway Advanced Edition ausgeführt wird. Diese Verbindungen sind sicherheitssensibel, weil sie zum Konfigurieren des Access Gateways und zum Gewähren oder Verweigern des Zugriffs auf Netzwerkressourcen unter Verwendung von Sitzungsrichtlinien verwendet werden.

Das Access Gateway setzt voraus, dass die richtigen Stammzertifikate installiert werden, die zum Signieren der Serverzertifikate verwendet werden. Weitere Informationen zu Stammzertifikaten finden Sie unter "Installieren von Stammzertifikaten auf dem Access Gateway" auf Seite 56.

So legen Sie fest, dass für interne Clientverbindungen Serverzertifikate vorhanden sein müssen

Aktivieren Sie auf der Registerkarte **Global Cluster Policies** unter **Select security options** die Option **Validate secure certificates for internal connections**.

Verwenden von Platzhalterzertifikaten

Das Access Gateway unterstützt die Überprüfung von Platzhalterzertifikaten für das Access Gateway Plug-in. Platzhalterzertifikate sind am Sternchen (*) in ihrem Namen erkennbar. Sie können eines der beiden folgenden Formate haben: **.meinefirma.com* oder *www*.meinefirma.com*. Bei Verwendung eines Platzhalterzertifikats können die Benutzer zwischen unterschiedlichen Webadressen wählen, z. B. http://www1.meinefirma.com oder http://www2.meinefirma.com. Durch die Verwendung eines Platzhalterzertifikats kann ein Zertifikat für mehrere Websites verwendet werden.

Beispiele für die Konfiguration des Netzwerkzugriffs

Nachdem Sie das Access Gateway installieren und für den Betrieb in Ihrer Netzwerkumgebung konfiguriert haben, können Sie den Benutzerzugriff auf die Server, Anwendungen und sonstigen Ressourcen im internen Netzwerk mit dem Administration Tool konfigurieren.

Das Konfigurieren des Benutzerzugriffs auf interne Netzwerkressourcen schließt die folgenden Schritte ein: Definieren zugänglicher Netzwerke für Split-Tunneling, Konfigurieren von Authentifizierung und Autorisierung, Erstellen von Benutzergruppen, Erstellen von lokalen Benutzern und Definieren der Zugriffssteuerungslisten (ACLs) für Benutzergruppen.

Hinweis: Eine Zugriffssteuerungsliste ist ein Richtliniensatz, mit der die Zugriffsstufe von Benutzern auf die Netzwerkressourcen festgelegt wird.

Das Access Gateway unterstützt verschiedene Authentifizierungs- und Autorisierungstypen, die sich in unterschiedlichen Kombinationen konfigurieren und mit Richtlinien verwenden lassen, um den Benutzerzugriff auf das interne Netzwerk zu steuern.

Aufgrund der Vielzahl von Optionen und Möglichkeiten bei der Konfiguration des Benutzerzugriffs auf das interne Netzwerk wird dieser Aspekt der Access Gateway-Konfiguration in vier verschiedenen Abschnitten dieses Handbuchs behandelt:

- Dieser Anhang enthält Beispielszenarien für den Benutzerzugriff und detaillierte Anweisungen, wie Sie das Access Gateway schrittweise zur Unterstützung der Zugriffsszenarios konfigurieren. Diese Szenarios sind keine Beispiele für echte Konfigurationen aus der Praxis, sondern vielmehr als eine Art Lernprogramm gedacht, damit Sie leichter verstehen, wie die im Administration Tool integrierten Funktionen zum Konfigurieren des Benutzerzugriffs zu verwenden sind.

  Nachdem Sie sich mit diesen Beispielen und den Grundkenntnissen zum Konfigurieren des Benutzerzugriffs vertraut gemacht haben, können Sie den Benutzerzugriff auf das Access Gateway in Ihrer Produktionsumgebung anhand der in den folgenden Kapiteln enthaltenen Informationen konfigurieren:

- Kapitel 6, "Konfigurieren der Authentifizierung und Autorisierung" : In diesem Kapitel werden die verschiedenen Authentifizierungs- und Autorisierungsoptionen und deren Konfiguration erläutert.
- Kapitel 7, "Konfigurieren von Netzwerkzugriff und Gruppenressourcen" : In diesem Kapitel wird die Arbeit mit Benutzergruppen, Netzwerkressourcen und verschiedenen Richtlinien zum Definieren von Zugriffssteuerungslisten auf dem Access Gateway beschrieben.
- Kapitel 8, "Konfigurieren von Benutzerverbindungen für das Citrix Access Gateway Plug-in" : In diesem Kapitel werden Clientverbindungen zum Access Gateway beschrieben.

Konfigurationsbeispiele

Bevor Sie sich die Beispiele in diesem Kapitel durchlesen, sollten Sie sich mit den Einstellungen auf drei Registerkarten des Administration Tools vertraut machen. Mit den Einstellungen auf diesen Registerkarten wird der Benutzerzugriff auf interne Netzwerkressourcen gesteuert:

- Global Cluster Policies
- Authentifizierung
- Access Policy Manager

Nachstehend finden Sie eine Liste der in diesem Kapitel beschriebenen Konfigurationsbeispiele für den Benutzerzugriff.

- Konfigurieren der LDAP-Authentifizierung und -Autorisierung: In diesem Beispiel wird schrittweise erläutert, wie ein Administrator den Zugriff auf interne Netzwerkressourcen in einer LDAP-Umgebung gewähren könnte.
- Erstellen von Gastkonten mit der Liste **Local Users**: In diesem Beispiel wird das Szenario für das Konfigurieren der LDAP-Authentifizierung und -Autorisierung erweitert, um das Konzept der lokalen Benutzer zu erläutern.
- Konfigurieren der lokalen Autorisierung: In diesem Beispiel wird das Konzept der lokalen Autorisierung erläutert, indem die im Szenario für das Erstellen von Gastkonten beschriebene Konfiguration mit der Liste **Local Users** geringfügig geändert wird.

Konfigurieren der LDAP-Authentifizierung und -Autorisierung

Dieses Beispiel veranschaulicht, wie ein Administrator mit den Einstellungen im Administration Tool den Benutzerzugriff konfigurieren könnte:

- Das Unternehmen verwendet nur ein LDAP-Verzeichnis als Benutzerrepository.
- Remotebenutzer, die für die Vertriebsabteilung arbeiten, müssen Zugriff auf einen E-Mail-Server, einen Webkonferenzserver, eine Webanwendung für den Vertrieb und mehrere Dateiserver im internen Netzwerk haben.
- Remotebenutzer, die für die technische Abteilung arbeiten, müssen Zugriff auf einen E-Mail-Server, einen Webkonferenzserver und mehrere Dateiserver im internen Netzwerk haben.
- Im internen Netzwerk sind zwar drei E-Mail-Server vorhanden; der Administrator möchte Remotebenutzern jedoch nur den Zugriff auf einen dieser E-Mail-Server gewähren.

Um den Zugriff auf die internen Netzwerkressourcen in diesem Szenario zu konfigurieren, führt der Administrator diese beiden grundlegenden Arbeitsschritte aus:

- Vorbereiten der Konfiguration von LDAP-Authentifizierung und -Autorisierung
- Konfigurieren des Access Gateways zur Unterstützung des Zugriffs auf die internen Netzwerkressourcen

Diese Arbeitsschritte werden im Folgenden jeweils näher erläutert.

Vorbereiten der Konfiguration von LDAP-Authentifizierung und -Autorisierung

Die Vorbereitung der Konfiguration von LDAP-Authentifizierung und -Autorisierung ist der erste Arbeitsschritt, den der Administrator beim Szenario für das Konfigurieren der LDAP-Authentifizierung und -Autorisierung vom ausführt.

Bei diesem Arbeitsschritt stellt der Administrator die Informationen zusammen, die für die Konfiguration des Access Gateways zur Unterstützung von LDAP-Authentifizierung und -Autorisierung erforderlich sind.

Dabei sind die folgenden Arbeitsschritte erforderlich:

- Festlegen, welche internen Netzwerke die jeweils gewünschten Ressourcen enthalten
- Festlegen, welche Benutzer aus den Abteilungen Vertrieb und Technik Remotezugriff benötigen
- Sammeln der LDAP-Verzeichnisinformationen

Festlegen, welche internen Netzwerke die gewünschten Ressourcen enthalten

Zum Vorbereiten der Konfiguration von LDAP-Authentifizierung und -Autorisierung muss der Administrator zuerst festlegen, welche internen Netzwerke die gewünschten Ressourcen enthalten.

Dabei legt der Administrator die Netzwerkpfade der Ressourcen fest, auf die Remotebenutzer Zugriff haben müssen. Im Folgenden werden noch einmal die Anforderungen wiederholt:

- Remotebenutzer, die für die Vertriebsabteilung arbeiten, müssen Zugriff auf einen E-Mail-Server, einen Webkonferenzserver, eine Webanwendung für den Vertrieb und mehrere Dateiserver im internen Netzwerk haben.
- Remotebenutzer, die für die technische Abteilung arbeiten, müssen Zugriff auf einen E-Mail-Server, einen Webkonferenzserver und mehrere Dateiserver im internen Netzwerk haben.
- Im internen Netzwerk sind zwar drei E-Mail-Server vorhanden; der Administrator möchte Remotebenutzern jedoch nur den Zugriff auf einen dieser E-Mail-Server gewähren.

Für diesen Arbeitsschritt wird angenommen, dass der Administrator die folgenden Informationen gesammelt hat:

- Der Webkonferenzserver, die E-Mail-Server und die Dateiserver, auf die Remotebenutzer aus den Abteilungen Vertrieb und Technik zugreifen müssen, befinden sich im Netzwerk 10.10.0.0/24.
- Der Server, auf dem die Webanwendung für den Vertrieb installiert ist, befindet sich im Netzwerk 10.60.10.0/24.
- Der einzelne E-Mail-Server, auf den Remotebenutzer zugreifen müssen, hat die IP-Adresse 10.10.25.50.

Festlegen, welche Benutzer aus den Abteilungen Vertrieb und Technik Remotezugriff benötigen

Zum Vorbereiten der Konfiguration von LDAP-Authentifizierung und -Autorisierung muss der Administrator im zweiten Arbeitsschritt festlegen, welche Benutzer aus den Abteilungen Vertrieb und Technik Remotezugriff benötigen.

Bevor ein Administrator das Access Gateway zur Unterstützung der Autorisierung mit einem LDAP-Verzeichnis konfigurieren kann, muss er verstehen, wie das Access Gateway den Autorisierungsvorgang mit Gruppen vornimmt.

Insbesondere muss der Administrator das Verhältnis zwischen der Gruppenmitgliedschaft eines Benutzers im LDAP-Verzeichnis und der Gruppenmitgliedschaft eines Benutzers auf dem Access Gateway verstehen.

Hinweis: Zur Unterstützung von Autorisierungstypen basiert das Access Gateway ähnlich wie RADIUS auf Benutzergruppen.

Wenn ein Benutzer in einem LDAP-Verzeichnis eine Verbindung zum Access Gateway herstellt, läuft die grundlegende Authentifizierung und Autorisierung in der folgenden Reihenfolge ab:

- Nachdem ein Benutzer seine Authentifizierungsinformationen vom LDAP-Verzeichnis eingegeben hat, sucht das Access Gateway nach diesem Benutzer im LDAP-Verzeichnis, überprüft die Anmeldeinformationen des Benutzers und meldet den Benutzer an.
- Nach der erfolgreichen Authentifizierung prüft das Access Gateway ein Attribut im Personeneintrag des LDAP-Verzeichnisses des Benutzers, um festzustellen, welchen LDAP-Verzeichnisgruppen dieser Benutzer angehört.

  Wenn das Access Gateway beispielsweise mit Microsoft Active Directory arbeitet, prüft das Access Gateway das Attribut "memberOf" im Personeneintrag, um festzustellen, welchen Gruppen ein Benutzer angehört.

  In diesem Beispiel wird angenommen, dass der Benutzer Mitglied der LDAP-Verzeichnisgruppe "Vertriebsaußendienst" ist.
- Dann sucht das Access Gateway nach einer auf der Registerkarte **Access Policy Manager** im Administration Tool konfigurierten Benutzergruppe, deren Name mit dem Namen einer LDAP-Verzeichnisgruppe übereinstimmt, der dieser Benutzer angehört.

  In diesem Beispiel sucht das Access Gateway nach der auf dem Access Gateway konfigurierten Benutzergruppe "Vertriebsaußendienst".

  Wenn das Access Gateway eine solche Benutzergruppe findet, erhält der Benutzer die der Benutzergruppe auf dem Access Gateway zugewiesenen Zugriffsberechtigungen (Autorisierung).

  In diesem Beispiel gewährt das Access Gateway Benutzern den Zugriff, der mit der Benutzergruppe "Vertriebsaußendienst" auf der Registerkarte **Access Policy Manager** im Administration Tool verknüpft sind.

Bevor der Administrator den Benutzern aus den Abteilungen Vertrieb und Technik den Zugriff auf interne Netzwerkressourcen über das Access Gateway gewähren kann, muss er also wissen, welchen LDAP-Verzeichnisgruppen diese

Benutzer angehören. Jetzt muss der Administrator in diesem Szenario einen der beiden Schritte in Bezug auf die Gruppenmitgliedschaft der Benutzer ausführen:

- Er muss die Gruppen im LDAP-Verzeichnis identifizieren, die sämtliche Mitglieder enthalten, für die Remotezugriff auf die internen Netzwerke erforderlich ist.
- Wenn keine Gruppe vorhanden ist, die alle betreffenden Mitglieder enthält, kann der Administrator neue Gruppen im LDAP-Verzeichnis erstellen und die betreffenden Mitglieder diesen Gruppen hinzufügen.

In diesem Beispiel wird davon ausgegangen, dass der Administrator die Gruppen "Vertriebsaußendienst" und "Außendiensttechniker" im LDAP-Verzeichnis erstellt und diesen Gruppen Benutzer aus den Abteilungen "Vertrieb" und "Technik" hinzufügt, die Remotezugriff auf die internen Netzwerkressourcen haben sollen.

Sammeln der LDAP-Verzeichnisinformationen

Zum Vorbereiten der Konfiguration von LDAP-Authentifizierung und -Autorisierung muss der Administrator als letzten Schritt die LDAP-Verzeichnisinformationen sammeln.

In diesem Beispiel verwendet das Unternehmen nur ein LDAP-Verzeichnis als Benutzerrepository.

Bevor der Administrator das Access Gateway für die Unterstützung von Authentifizierung und Autorisierung mit einem LDAP-Verzeichnis konfigurieren kann, muss er Informationen über das LDAP-Verzeichnis sammeln. Mit diesen Informationen wird das Access Gateway später zum Herstellen einer Verbindung zum LDAP-Verzeichnis konfiguriert, um nach Benutzer- und Gruppennamen zu suchen.

Hinweis: Welche Informationen zum Konfigurieren eines bestimmten Authentifizierungs- oder Autorisierungstyps erforderlich sind, finden Sie in der *Access Gateway Standard Edition Installationscheckliste*. Sie können auch im Administrator Tool auf die Registerkarte **Authentication** klicken und einen Testauthentifizierungsbereich erstellen, der die Authentifizierungs- und Autorisierungstypen enthält, die unterstützt werden müssen. Sammeln Sie die erforderlichen Informationen, um die Felder für die gewählten Authentifizierungs- und Autorisierungstypen auszufüllen.

In diesem Arbeitsschritt sammelt der Administrator die folgenden Informationen über das LDAP-Verzeichnis.

- **IP-Adresse des LDAP-Servers:** Die IP-Adresse des Computers, auf dem der LDAP-Server ausgeführt wird.
- **LDAP-Serverport:** Der Port, auf dem der LDAP-Server Verbindungen abhört. Der Standardport für LDAP-Verbindungen ist Port 389.
- **LDAP-Administrator-DN und LDAP-Administratorkennwort:** Wenn für den Zugriff von Anwendungen auf das LDAP-Verzeichnis eine Authentifizierung erforderlich ist, muss der Administrator den Namen des Benutzerkontos, mit dem das Access Gateway diese Authentifizierung vornehmen soll, sowie das mit diesem Konto verknüpfte Kennwort kennen.
- **LDAP-Basis-DN:** Das Basisobjekt des Verzeichnisses (oder die Verzeichnisebene), in dem Benutzernamen gespeichert werden. Auf dieser Verzeichnisebene müssen alle Remotebenutzer einen Personeneintrag haben. Nachstehend einige Beispielwerte:

  ou=Benutzer,dc=ace,dc=com

  cn=Users,dc=ace,dc=com
- **LDAP-Attribut für Serveranmeldung:** Das Attribut eines Personeneintrags im LDAP-Verzeichnis, das einen Benutzernamen enthält. Die folgende Tabelle enthält Beispiele für die Benutzernamen-Attributfelder für verschiedene LDAP-Verzeichnisse:

LDAP-Server	**Benutzerattribut**	**Groß-/ Kleinschreibung relevant**
Microsoft Active Directory-Server	sAMAccountName	Nein
Novell eDirectory	cn	Ja
IBM Directory Server	uid	
Lotus Domino	CN	
Sun ONE-Verzeichnis (früher iPlanet)	uid oder cn	Ja

- **LDAP-Gruppenattribut:** Das Attribut des Personeneintrags eines Benutzers, das eine Liste der Gruppen enthält, denen dieser Benutzer angehört, z. B. "memberOf". Das LDAP-Gruppenattribut wird nur bei der LDAP-Autorisierung verwendet.

Jetzt hat der Administrator alle notwendigen Vorbereitungsschritte für die Konfiguration der LDAP-Authentifizierung und -Autorisierung abgeschlossen. Danach stehen dem Administrator die folgenden Informationen zur Verfügung:

- Die exakten Netzwerkpfade aller Netzwerkressourcen, auf die Remotebenutzer aus den Abteilungen Vertrieb und Technik zugreifen müssen.
- Die Namen der Benutzergruppen im LDAP-Verzeichnis mit den Benutzern aus den Abteilungen Vertrieb und Technik, die Remotezugriff benötigen (bei diesem Beispiel "Vertriebsaußendienst" und "Außendiensttechniker")
- Die exakten LDAP-Verzeichnisinformationen, die zum Konfigurieren des Access Gateways für die Arbeit mit dem LDAP-Verzeichnis erforderlich sind.

Anhand dieser Informationen kann der Administrator nun das Access Gateway konfigurieren, um den Benutzern aus den Abteilungen Vertrieb und Technik Zugriff auf die internen Netzwerkressourcen zu gewähren.

Konfigurieren des Access Gateways zur Unterstützung des Zugriffs auf die internen Netzwerkressourcen

Die Konfiguration des Access Gateways zur Unterstützung des Zugriffs auf die internen Netzwerkressourcen ist der letzte Arbeitsschritt, den der Administrator bei der Konfiguration der LDAP-Authentifizierung und -Autorisierung ausführt.

Dabei verwendet der Administrator die im vorigen Arbeitsschritt gesammelten Informationen, um die Einstellungen im Administration Tool zu konfigurieren, damit Remotebenutzer auf die internen Netzwerkressourcen zugreifen können.

Dabei sind die folgenden fünf Arbeitsschritte erforderlich:

- Konfigurieren der zugänglichen Netzwerke
- Erstellen eines LDAP-Authentifizierungsbereichs
- Erstellen der entsprechenden Gruppen auf dem Access Gateway
- Erstellen und Zuweisen von Netzwerkressourcen für die Benutzergruppen
- Erstellen einer Anwendungsrichtlinie für den E-Mail-Server

Diese Schritte werden im Folgenden genauer erläutert.

Konfigurieren der zugänglichen Netzwerke

Das Konfigurieren der zugänglichen Netzwerke ist der erste von fünf Arbeitsschritten, die der Administrator ausführt, um beim Konfigurationsszenario für die LDAP-Authentifizierung und -Autorisierung den Zugriff auf die internen Netzwerkressourcen zu konfigurieren.

In diesem Arbeitsschritt gibt der Administrator die internen Netzwerke mit den Netzwerkressourcen an, auf die Benutzer über den Access Gateway Plug-in zugreifen müssen.

Im vorigen Arbeitsschritt hat der Administrator festgelegt, dass Remotebenutzer aus den Abteilungen Vertrieb und Technik auf die in die Ressourcen in folgenden internen Netzwerken Zugriff haben müssen:

- Webkonferenzserver, Dateiserver und E-Mail-Server in Netzwerk 10.10.0.0/24
- Server mit der Webanwendung für den Vertrieb in Netzwerk 10.60.10.0/24

Der Administrator legt diese Netzwerke als zugängliche Netzwerke fest. Durch Festlegen der zugänglichen Netzwerke kann das Access Gateway Plug-in Split-Tunneling unterstützen.

Wenn sich Benutzer am Access Gateway anmelden, leitet das Access Gateway diese Netzwerkliste an das Access Gateway Plug-in auf dem Computer der Benutzer weiter. Das Access Gateway Plug-in verwendet die Liste als Filter, um festzulegen, welche ausgehenden Pakete an das Access Gateway und welche Pakete anderweitig weitergeleitet werden sollen. Das Access Gateway Plug-in leitet nur die für das Access Gateway bestimmten Pakete über den sicheren Tunnel an das Access Gateway weiter.

Hinweis: Wenn Split-Tunneling nicht unterstützt werden soll, erübrigt sich das Konfigurieren der zugänglichen Netzwerke.

So konfigurieren Sie zugängliche Netzwerke

1. Öffnen Sie das Administration Tool.
2. Klicken Sie auf die Registerkarte **Global Cluster Policies**.
3. Wählen Sie ggf. unter **Access options** die Option **Enable split tunneling**.
4. Geben Sie im Feld **Accessible networks** alle internen Netzwerke ein, auf die das Access Gateway zugreifen muss. Trennen Sie die einzelnen Netzwerkeinträge durch ein Leerzeichen oder einen Zeilenumbruch voneinander. Bei diesem Zugriffsszenario würde der Administrator die folgenden Eingaben machen:

   10.10.0.0/24

   10.60.10.0/24
5. Wählen Sie unter **Advanced options** die Option **Enable logon page authentication**. Bei dieser Einstellung müssen sich die Benutzer authentifizieren, wenn sie über einen Webbrowser auf das Access Gateway zugreifen.

Zur Vereinfachung dieses Beispiels wird angenommen, dass der Administrator alle anderen Kontrollkästchen auf der Registerkarte **Global Cluster Policies** deaktiviert. Weitere Informationen über Split-Tunneling finden Sie unter "Aktivieren von Split-Tunneling und zugänglichen Netzwerken" auf Seite 114. Weitere Informationen über die Einstellung **Deny Access without access control list** finden Sie unter "Zugriffssteuerungslisten" auf Seite 92.

Erstellen eines LDAP-Authentifizierungs- und Autorisierungsbereichs

Das Erstellen eines LDAP-Authentifizierungs- und -Autorisierungsbereichs ist der zweite von fünf Arbeitsschritten, die der Administrator zum Konfigurieren des Zugriffs auf die internen Netzwerkressourcen ausführt.

In diesem Szenario sind alle Benutzer aus den Abteilungen "Vertrieb" und "Technik" in dem LDAP-Verzeichnis aufgeführt.

Zum Authentifizieren der in einem LDAP-Verzeichnis aufgeführten Benutzer muss der Administrator einen Authentifizierungsbereich erstellen, der die LDAP-Authentifizierung unterstützt.

Um den in LDAP-Verzeichnisgruppen aufgeführten Benutzern Zugriff auf die internen Netzwerkressourcen zu gestatten, wählt der Administrator die LDAP-Authentifizierung als Autorisierungstyp für den Bereich aus.

Da sich Benutzer über das LDAP-Verzeichnis authentifizieren, richtet der Administrator den Authentifizierungsbereich "Default" als Standardbereich zur Unterstützung der LDAP-Authentifizierung und -Autorisierung ein.

Zum Einrichten des Standardbereichs zur Unterstützung der LDAP-Authentifizierung löscht der Administrator zuerst den vorhandenen Standardbereich (Default) und erstellt dann sofort einen neuen Standardbereich, der LDAP-Authentifizierung unterstützt. Dieser neue Bereich enthält die Adresse, den Port und andere LDAP-Verzeichnisinformationen, die das Access Gateway zum Herstellen einer Verbindung zum LDAP-Verzeichnisserver und zum Suchen nach Namen im Verzeichnis benötigt.

Hinweis: Der auf dem Access Gateway vorhandene Standardbereich wird für die lokale Authentifizierung konfiguriert. Durch das Löschen des vorhandenen Standardbereichs und das Erstellen eines neuen Standardbereichs für LDAP erleichtert der Administrator den Anmeldevorgang für den Endbenutzer. Benutzer, die sich über den Standardbereich authentifizieren, müssen den Bereichsnamen nicht als Bestandteil ihrer Anmeldeinformationen eingeben. Weitere Informationen über Bereiche (realms), Authentifizierung und Autorisierung finden Sie unter "Konfigurieren der Authentifizierung und Autorisierung" auf Seite 71.

Für diesen Arbeitsschritt muss der Administrator die im vorigen Arbeitsschritt "Sammeln der LDAP-Verzeichnisinformationen" gesammelten Informationen griffbereit haben.

So löschen Sie den vorhandenen Standardbereich (Default) und erstellen einen neuen Standardbereich, der LDAP-Authentifizierung und -Autorisierung unterstützt

1. Klicken Sie im Access Gateway Administration Tool auf die Registerkarte **Authentication**.
2. Öffnen Sie das Fenster für den Bereich "Default".
3. Wählen Sie im Menü **Action** den Befehl **Remove "Default" realm**.

   Es wird eine Warnmeldung angezeigt.
4. Klicken Sie auf **Ja**.
5. Geben Sie im Feld **Realm name** den Namen "Default" ein.
6. Wählen Sie **One Source** und klicken Sie auf **Add**.
7. Aktivieren Sie im Dialogfeld **Select Authentication Type** die Option **LDAP authentication** und klicken Sie dann auf **OK**.

   Dann wird das Fenster für den neuen Standardbereich geöffnet.

8. Füllen Sie im Fenster für den neuen Standardbereich auf der Registerkarte **Authentication** die erforderlichen Felder aus, um dem Access Gateway Zugriff auf den LDAP-Server zu ermöglichen. (Verwenden Sie hierfür die im vorigen Arbeitsschritt "Sammeln der LDAP-Verzeichnisinformationen" gesammelten Informationen.)
9. Klicken Sie auf die Registerkarte **Authorization**.
10. Wählen Sie unter **Authorization type** die Option **LDAP authorization**.
11. Füllen Sie auf der Registerkarte **Authorization** die erforderlichen Felder aus, um dem Access Gateway Zugriff auf den LDAP-Server zu ermöglichen.
12. Klicken Sie auf **Submit**.

Weitere Informationen zum Erstellen von Bereichen finden Sie unter "Konfigurieren des Bereichs "Default"" auf Seite 75.

Erstellen der entsprechenden Gruppen auf dem Access Gateway

Das Erstellen der entsprechenden Gruppen auf dem Access Gateway ist der dritte von fünf Arbeitsschritten, die der Administrator ausführt, um beim Konfigurationsszenario für die LDAP-Authentifizierung und -Autorisierung den Zugriff auf die internen Netzwerkressourcen zu konfigurieren.

In diesem Schritt erstellt der Administrator Benutzergruppen auf dem Access Gateway, deren Namen mit den Namen der Gruppen übereinstimmen, die der Administrator im LDAP-Verzeichnis gefunden oder erstellt hat.

In einem vorigen Arbeitsschritt hat der Administrator die LDAP-Verzeichnisgruppen "Vertriebsaußendienst" und "Außendiensttechniker" im LDAP-Verzeichnis erstellt.

In diesem Schritt muss der Administrator nun die Benutzergruppen "Vertriebsaußendienst" und "Außendiensttechniker" auf dem Access Gateway erstellen.

So erstellen Sie Benutzergruppen auf dem Access Gateway

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Klicken Sie mit der rechten Maustaste im linken Bereich auf **User Groups** und klicken Sie dann auf **New Group**.

   Geben Sie im Feld **Group Name** einen Namen ein, dessen Schreibweise (Groß- und Kleinschreibung) genau mit dem Namen einer LDAP-Verzeichnisgruppe aus dem vorigen Schritt übereinstimmt.

   Geben Sie beispielsweise "Vertriebsaußendienst" ein und klicken Sie dann auf **OK**.
3. Jetzt wird das Eigenschaften-Dialogfeld der Gruppe angezeigt. Es enthält mehrere Registerkarten. Zur Vereinfachung dieses Beispiels akzeptieren Sie alle Standardeinstellungen für die Gruppeneigenschaften und klicken Sie auf **OK**.

   Die Gruppeneigenschaften enthalten zusätzliche Einstellungen, die sich auf den Benutzerzugriff auswirken. Weitere Informationen zu Gruppeneigenschaften und zum Erstellen von lokalen Gruppen finden Sie unter "Konfigurieren von Benutzergruppen" auf Seite 115.

Erstellen und Zuweisen von Netzwerkressourcen für die Benutzergruppen

Das Erstellen und Zuweisen von Netzwerkressourcen für die Benutzergruppen ist der vierte von fünf Arbeitsschritten, die der Administrator ausführt, um beim Konfigurationsszenario für die LDAP-Authentifizierung und -Autorisierung den Zugriff auf die internen Netzwerkressourcen zu konfigurieren.

In diesem Schritt gibt der Administrator an, auf welche Netzwerkressourcen (Netzwerksegmente oder einzelne Computer) Benutzer zugreifen dürfen, und weist diese Ressourcen dann den Benutzergruppen auf dem Access Gateway zu.

Dabei führt der Administrator folgende Schritte aus:

- Erstellen der Netzwerkressource "Vertriebsressource" und Zuweisen dieser Ressource zur Benutzergruppe "Vertriebsaußendienst"
- Erstellen der Netzwerkressource "Technische Ressource" und Zuweisen dieser Ressource zur Benutzergruppe "Außendiensttechniker"

Erstellen und Zuweisen von Netzwerkressourcen für die Benutzer im Vertrieb

In diesem Abschnitt wird kurz erläutert, wie der Administrator eine Netzwerkressource für die Benutzer im Vertrieb erstellt und diesen Benutzern zuweist.

Wie bereits oben erwähnt, benötigen die Benutzer im Vertrieb Zugriff auf die folgenden Systeme:

- E-Mail-Server, Webkonferenzserver und mehrere Dateiserver im Netzwerk 10.10.0.0/24
- Webanwendung für den Vertrieb im Netzwerk 10.60.10.0/24

So erstellen Sie die Netzwerkressource "Vertriebsressource" für die Benutzer im Vertrieb

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Klicken Sie mit der rechten Maustaste im linken Bereich auf **Network Resources** und klicken Sie dann auf **New Network Resource**.
3. Geben Sie "Vertriebsressource" als Namen für die Netzwerkressource ein und klicken Sie auf **OK**.
4. Geben Sie im Feld **Network and subnet mask** die beiden IP-Adress-/Subnetzpaare für die Ressourcen ein. Trennen Sie diese IP-Adress-/Subnetzpaare jeweils durch ein Leerzeichen voneinander:

   10.10.0.0/24 10.60.10.0/24
5. Zur Vereinfachung dieses Beispiels übernimmt der Administrator die Standardwerte für die anderen Einstellungen im Eigenschaften-Dialogfeld der Netzwerkressource und klickt auf **OK**.

Nach dem Erstellen dieser Netzwerkressource geht der Administrator wie nachstehend beschrieben vor, um diese Netzwerkressource der Zugriffssteuerungsliste für die Benutzergruppe "Vertriebsaußendienst" hinzuzufügen.

1. Klicken Sie im Access Gateway Administration Tool auf die Registerkarte **Access Policy Manager**.
2. Erweitern Sie im linken Bereich den Eintrag **User Groups** und dann die Benutzergruppe "Vertriebsaußendienst".
3. Erweitern Sie im rechten Bereich den Eintrag **Network Resources**.
4. Klicken Sie auf die Netzwerkressource "Vertriebsressource" und ziehen Sie diese im linken Bereich auf den Knoten **Network Policies** unter der Benutzergruppe "Vertriebsaußendienst".

   Hierdurch gewährt der Administrator den mit dieser Benutzergruppe verknüpften Benutzern Zugriff auf die Systeme, die in der Netzwerkressource "Vertriebsressource" definiert sind.

Hinweis: Im obigen Arbeitsschritt hat der Administrator die Netzwerkressource "Vertriebsressource" der Zugriffssteuerungsliste der Benutzergruppe "Vertriebsaußendienst" zugewiesen. Zugriffssteuerungslisten werden vom Administrator auf dem Access Gateway durch Hinzufügen der mit der Benutzergruppe verknüpften Netzwerk-, Anwendungs- und Endpunktrichtlinien erstellt. Die Zugriffssteuerungsliste besteht aus allen Richtlinien, die einer Benutzergruppe auf dem Access Gateway zugewiesen sind.

Erstellen und Zuweisen von Netzwerkressourcen für die Benutzer im Bereich "Technik"

In diesem Abschnitt wird kurz erläutert, wie der Administrator eine Netzwerkressource für die Benutzer im Bereich "Technik" erstellt und diesen Benutzern zuweist. Abgesehen davon, dass der Administrator den Benutzern im Bereich "Technik" keinen Zugriff auf die Webanwendung für "Vertrieb" in Netzwerk 10.60.10.0/24 gewährt, ist die Vorgehensweise im Wesentlichen identisch mit dem vorigen Arbeitsschritt für die Benutzer im "Vertrieb".

Wie bereits oben erwähnt, müssen die Techniker auf einen Webkonferenzserver, einen E-Mail-Server und mehrere Dateiserver zugreifen. Alle diese Server sind im Netzwerk 10.10.0.0/24.

So gewähren Sie den Benutzern aus dem Bereich "Technik" Zugriff auf das Netzwerk

1. Erstellen Sie im rechten Bereich der Registerkarte Access Policy Manager im Access Gateway Administration Tool eine neue Netzwerkressource "Technikerressourcen". Geben Sie beim Erstellen dieser Ressource nur das Netzwerk 10.10.0.0/24 an.
2. Erweitern Sie im linken Bereich die Benutzergruppe "Außendiensttechniker".
3. Ziehen Sie die Netzwerkressource "Technikerressourcen" aus dem rechten Bereich der Registerkarte **Access Policy Manager** auf **Network Policies** der Gruppe "Außendiensttechniker" im linken Bereich.

   Jetzt ist die Netzwerkressource "Technikerressourcen" ein Bestandteil der Zugriffssteuerungsliste für die Gruppe "Außendiensttechniker".

Hinweis: In komplexeren Umgebungen muss der Zugriff u. U. auf ein bestimmtes Segment eines größeren Netzwerks eingeschränkt werden. Beispiel: Ein Administrator muss den Zugriff auf das Netzwerk 10.0.20.x verweigern, doch den Zugriff auf alles andere im Netzwerk 10.0.x.x zulassen. Der Administrator erstellt eine Netzwerkressource für das Netzwerk 10.0.20.x und eine Netzwerkressource für das Netzwerk 10.0.x.x und weist der Benutzergruppe beide Netzwerkressourcen zu. Dann klickt der Administrator jeweils mit der rechten Maustaste auf die beiden Ressourcen, um den Zugriff auf die Ressource im Netzwerk 10.0.20.x zu verweigern und den Zugriff auf die Ressource im Netzwerk 10.0.x.x zuzulassen. In solchen Fällen konfigurieren Sie zuerst die Richtlinie, wonach der Zugriff auf 10.0.20.x verweigert wird, und dann die Richtlinie, wonach der Zugriff auf das Netzwerk 10.0.x.x zugelassen wird. Konfigurieren Sie die Richtlinie mit den größten Einschränkungen stets zuerst und die Richtlinie mit den geringsten Einschränkungen zuletzt.

Erstellen einer Anwendungsrichtlinie für einen E-Mail-Server

Das Erstellen einer Anwendungsrichtlinie für einen E-Mail-Server ist der letzte von fünf Arbeitsschritten, die der Administrator ausführt, um beim Konfigurationsszenario für die LDAP-Authentifizierung und -Autorisierung den Zugriff auf die internen Netzwerkressourcen zu konfigurieren.

In diesem Beispiel sind im Netzwerk 10.10.0.0/24 drei E-Mail-Server installiert, wobei der Administrator den Remotebenutzern aus den Bereichen "Vertrieb" und "Technik" allerdings nur Zugriff auf einen dieser E-Mail-Server gewähren möchte. Der E-Mail-Server, auf den Remotebenutzer zugreifen müssen, hat die IP-Adresse 10.10.25.50/32.

Damit die Benutzer nur auf einen E-Mail-Server zugreifen können, erstellt der Administrator eine Anwendungsrichtlinie auf dem Access Gateway, nach der die Benutzer nur auf die E-Mail-Anwendung auf dem E-Mail-Server 10.10.25.50/32 zugreifen können.

Hinweis: Mit Anwendungsrichtlinien legen Administratoren fest, dass eine Clientanwendung auf einen bestimmten internen Server zugreifen oder ein Clientgerät bestimmte Anforderungen erfüllen muss, bevor der Zugriff auf einen internen Server zulässig ist.

Um eine Anwendungsrichtlinie zu erstellen, die den E-Mail-Clientzugriff auf einen Server einschränkt, muss der Administrator drei Schritte ausführen:

- Erstellen einer Netzwerkressource, die nur den E-Mail-Server umfasst
- Erstellen einer Anwendungsrichtlinie, mit der die E-Mail-Anwendung auf dem E-Mail-Server angegeben wird, und Zuweisen der Netzwerkressource mit dem E-Mail-Server zu dieser Anwendungsrichtlinie
- Zuweisen der Anwendungsrichtlinie zu den Benutzergruppen im Access Gateway

In diesem Beispiel erstellt der Administrator eine Netzwerkressource "E-Mail-Server", die nur die IP-Adresse 10.10.25.50/32 (den E-Mail-Server) enthält. Dann erstellt der Administrator eine Anwendungsrichtlinie "E-Mail-Anwendungsrichtlinie", in der die E-Mail-Anwendung angegeben ist, auf die Remotebenutzer zugreifen können. Der Administrator weist dieser Anwendungsrichtlinie die Netzwerkressource "E-Mail-Server" zu.

Danach fügt der Administrator den Gruppen "Vertriebsaußendienst" und "Außendiensttechniker" die "E-Mail-Anwendungsrichtlinie" zu. Durch das Hinzufügen der Richtlinie zu diesen Gruppen ist gewährleistet, dass diese Gruppen stets auf die E-Mail-Anwendung auf dem vom Administrator in der Anwendungsrichtlinie angegebenen E-Mail-Server zugreifen.

So implementieren Sie die Anwendungsrichtlinie für den E-Mail-Server

1. Erstellen Sie im rechten Bereich auf der Registerkarte **Access Policy Manager** im Access Gateway Administration Tool eine neue Netzwerkressource "E-Mail-Server". Geben Sie für diese Netzwerkressource nur die IP-Adresse des E-Mail-Servers an, auf den die Benutzer zugreifen dürfen (z. B. 10.10.25.50/32). Diese Vorgehensweise ist im Wesentlichen identisch mit den vorigen Arbeitsschritten, bei denen die Netzwerkressourcen für die Benutzer in den Bereichen "Vertrieb" und "Technik" definiert wurden.
2. Klicken Sie mit der rechten Maustaste im rechten Bereich auf **Application Policies** und klicken Sie dann auf **New Application Policy**.
3. Geben Sie im Feld **Application Resource Name** "E-Mail-Anwendungsrichtlinie" ein und klicken Sie auf **OK**.
4. Suchen und markieren Sie die E-Mail-Anwendung, die auf dem Server mit der IP-Adresse 10.10.25.50/32 ist.

   Im Feld MD5 wird automatisch die Binärsumme der Anwendung eingetragen.
5. Klicken Sie im linken Bereich auf die soeben erstellte Netzwerkressource "E-Mail-Server" und ziehen Sie diese auf **Application network policies** unter dem Eintrag **Application Policies** im rechten Bereich und klicken auf **OK**.
6. Erweitern Sie im linken Bereich die Benutzergruppen "Vertriebsaußendienst" und "Außendiensttechniker".
7. Klicken Sie im rechten Bereich unter **Application Policies** auf die "E-Mail-Anwendungsrichtlinie" und ziehen Sie diese auf Application Policies unter der Benutzergruppe "Vertriebsaußendienst" im linken Bereich, sodass die Anwendungsrichtlinie ein Bestandteil der Zugriffssteuerungsliste für Außendienstmitarbeiter im Vertrieb ist.
8. Klicken Sie im rechten Bereich unter Application Policies auf die "E-Mail-Anwendungsrichtlinie" und ziehen Sie diese auf "Application Policies" unter der Benutzergruppe "Außendiensttechniker" im linken Bereich, sodass die Anwendungsrichtlinie ein Bestandteil der Zugriffssteuerungsliste für Außendiensttechniker ist.

Hinweis: Bei der oben beschriebenen Vorgehensweise könnte der Administrator der Anwendungsrichtlinie auch eine anwendungsspezifische Endpunktrichtlinie hinzufügen, wonach jedes Clientgerät beim Zugriff auf den E-Mail-Server bestimmte Anforderungen erfüllen muss. Weitere Informationen hierzu finden Sie unter "Festlegen von Anwendungsrichtlinien" auf Seite 126.

Mit diesen Arbeitsschritten ist das Szenario für die Konfiguration der LDAP-Authentifizierung und -Autorisierung abgeschlossen. Danach hat der Administrator Folgendes konfiguriert:

- Benutzer können sich über ihre LDAP-Anmeldeinformationen bei dem LDAP-Verzeichnis authentifizieren, das im Authentifizierungsbereich "Default" angegeben ist.
- Auf Basis ihrer Gruppenmitgliedschaft im LDAP-Verzeichnis und auf dem Access Gateway dürfen Benutzer auf die internen Netzwerkressourcen zugreifen.

  Nur Benutzer, die Mitglied der Gruppe "Vertriebsaußendienst" oder "Außendiensttechniker" sind, dürfen auf Ressourcen im internen Netzwerk zugreifen. (Beide Gruppen müssen jeweils im LDAP-Verzeichnis und auf dem Access Gateway vorhanden sein.)
- Benutzer der Gruppe "Vertriebsaußendienst" dürfen auf den Webkonferenzserver und die Dateiserver im Netzwerk 10.10.0.0/24 sowie auf die Webanwendung für den Vertrieb im Netzwerk 10.60.10.0/24 zugreifen.

  Die Benutzer aus dem Bereich "Vertrieb" können zwar auf die E-Mail-Anwendung auf dem Server mit der IP-Adresse 10.10.25.50, jedoch nicht auf die E-Mail-Anwendung auf anderen E-Mail-Servern in den zugelassenen Netzwerken zugreifen.

  Die Benutzer aus dem Bereich "Vertrieb" können auch auf andere Netzwerkressourcen zugreifen, die in den beiden zugelassenen Netzwerken sind.
- Benutzer der Gruppe "Außendiensttechniker" dürfen auf den Webkonferenzserver und die Dateiserver im Netzwerk 10.10.0.0/24 (und auf andere in diesem Netzwerk befindliche Netzwerkressourcen) zugreifen.

  Die Benutzer aus dem Bereich "Technik" können zwar auch auf die E-Mail-Anwendung auf dem Server mit der IP-Adresse 10.10.25.50, jedoch nicht auf die E-Mail-Anwendung auf anderen E-Mail-Servern in den zugelassenen Netzwerken zugreifen.

Nähere Informationen darüber, worin der Zweck von lokalen Benutzern auf dem Access Gateway besteht und wie die Authentifizierung und Autorisierung für lokale Benutzer zu ermöglichen ist, finden Sie unter"Szenario für das Erstellen von Gastkonten mit der Liste "Local Users"" auf Seite 262.

Szenario für das Erstellen von Gastkonten mit der Liste "Local Users"

Dieses Beispiel veranschaulicht die Funktionsweise von lokalen Benutzern auf dem Access Gateway und erläutert eine Methode, mit der ein Administrator die Authentifizierung und Autorisierung für lokale Benutzer unterstützen kann.

In dem zuvor beschriebenen Beispiel wurden Benutzer anhand ihrer Anmeldeinformationen für das LDAP-Verzeichnis und ihrer Gruppenmitgliedschaft authentifiziert und autorisiert.

Administratoren können auch eine Liste mit lokalen Benutzern auf dem Access Gateway erstellen und das Access Gateway so konfigurieren, dass diesen Benutzern Authentifizierungs- und Autorisierungsdienste zur Verfügung stehen. Diese Liste lokaler Benutzer wird in einer Datenbank auf dem Access Gateway, also nicht in einem externen Verzeichnis, verwaltet.

Lokale Benutzer eignen sich insbesondere, wenn der Administrator einen der folgenden Schritte ausführen möchte:

- Gewähren von Zugriff für Benutzer, die in keinem Verzeichnis für die Authentifizierung aufgeführt sind
- Gewähren von Zugriff für Benutzer, die in einem Verzeichnis aufgeführt sind, zu dem das Access Gateway keine Verbindung herstellt
- Gewähren bestimmter Zugriffsrechte auf die internen Netzwerkressourcen für einen kleinen Benutzerkreis, ohne für diese Benutzer eine neue Gruppe im Verzeichnis erstellen zu müssen

Bei diesem Beispiel wird von Folgendem ausgegangen:

- Silvio Branco und Lisa Marth sind Berater, die nicht für das Unternehmen arbeiten und auch nicht im Authentifizierungsverzeichnis aufgeführt sind.
- Silvio Branco und Lisa Marth müssen Remotezugriff auf den Webkonferenzserver im internen Netzwerk haben, damit sie an Konferenzen mit Benutzern aus den Bereichen "Vertrieb" und "Technik" teilnehmen können, die Angestellte der Organisation sind.
- Der Administrator hat die weiter oben in diesem Kapitel beschriebene LDAP-Authentifizierung und -Autorisierung bereits konfiguriert, sodass Benutzer aus den Bereichen "Vertrieb" und "Technik" auf den Webkonferenzserver zugreifen können.
- Der Webkonferenzserver hat die IP-Adresse 10.10.50.60.

Hinweis: In diesem Beispiel werden Silvio Branco und Lisa Marth als Gastbenutzer angesehen, weil sie keine Angestellten des Unternehmens und auch nicht in einem Authentifizierungsverzeichnis aufgeführt sind.

Um Silvio Branco und Lisa Marth Zugriff auf den Webkonferenzserver zu gewähren, führt der Administrator die folgenden drei Schritte aus:

- Erstellen eines Authentifizierungsbereichs für Gastbenutzer
- Erstellen von lokalen Benutzern
- Erstellen und Zuweisen einer Netzwerkressource für die Standardbenutzergruppe "Default" auf dem Access Gateway

Erstellen eines Authentifizierungsbereichs für Gastbenutzer

Das Erstellen eines Authentifizierungsbereichs für Gastbenutzer ist der erste von drei Arbeitsschritten, die der Administrator beim Szenario für das Erstellen von Gastkonten mit der Liste **Local Users** ausführt.

Beim vorigen Szenario für die Konfiguration von LDAP-Authentifizierung und -Autorisierung hat der Administrator einen Standardauthentifizierungsbereich (Default) erstellt, um die Authentifizierung und Autorisierung der in einem LDAP-Verzeichnis aufgeführten Benutzer zu unterstützen.

Da Silvio Branco und Lisa Marth nicht im LDAP-Verzeichnis aufgeführt sind, erstellt der Administrator einen separaten Authentifizierungsbereich für sie, der Folgendes unterstützt:

- **Lokale Authentifizierung:** Diese Option in einem Authentifizierungsbereich gewährleistet, dass Benutzer anhand einer Liste **Local Users** auf dem Access Gateway und nicht auf Basis eines externen Verzeichnisses authentifiziert werden.
- **Keine Autorisierung:** Diese Option in einem Authentifizierungsbereich gewährleistet, dass Benutzern dieses Bereichs die mit der Benutzergruppe "Default" auf dem Access Gateway verknüpften Zugriffsrechte gewährt werden.

So erstellen Sie einen Authentifizierungsbereich für die Gastbenutzer

1. Klicken Sie im Access Gateway Administration Tool auf die Registerkarte **Authentication**.
2. Geben Sie im Feld **Realm name** den Namen Gast ein.
3. Wählen Sie **One Source** und klicken Sie auf **Add**.
4. Aktivieren Sie im Dialogfeld **Select Authentication Type** unter **Authentication type** die Option **Local authentication only** und klicken Sie dann auf **OK**.
5. Aktivieren Sie auf der Registerkarte **Authorization** die Option **No authorization**.
6. Klicken Sie auf **Submit**.

Hinweis: Wenn der Gästebereich nicht der Standardbereich ist, müssen sich Benutzer mit dem Bereichsnamen anmelden, z B. *Gast/Benutzername*.

Erstellen lokaler Benutzer

Das Erstellen von lokalen Benutzern ist der zweite von drei Arbeitsschritten, die der Administrator beim Szenario für das Erstellen von Gastkonten mit der Liste **Local Users** ausführt.

Bei diesem Arbeitsschritt erstellt der Administrator lokale Benutzerkonten für Silvio Branco und Lisa Marth auf dem Access Gateway und gibt beiden Benutzern jeweils ein Kennwort.

So fügen Sie lokale Benutzer hinzu

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Klicken Sie mit der rechten Maustaste auf **Local Users** und wählen Sie dann die Option **New User**.
3. Geben Sie im Feld **User Name** Lisa Marth ein.
4. Geben Sie in den Feldern **Password** und **Verify Password** ein Kennwort für Lisa Marth ein und klicken Sie auf **OK**.
5. Wiederholen Sie die Schritte 2 bis 4, um ein lokales Benutzerkonto für Silvio Branco zu erstellen.

Erstellen und Zuweisen einer Netzwerkressource für die Standardbenutzergruppe

Das Erstellen und Zuweisen einer Netzwerkressource für die Standardbenutzergruppe **Default** ist der letzte von drei Arbeitsschritten beim Szenario für das Erstellen von Benutzerkonten mit der Liste Local Users.

Bei diesem Schritt erstellt der Administrator eine Netzwerkressource, in der nur der Webkonferenzserver angegeben ist, und weist dann diese Ressource der Benutzergruppe "Default" zu.

1. Erstellen Sie im rechten Bereich der Registerkarte **Access Policy Manager** im Administration Tool die neue Netzwerkressource "Gastressource". Geben Sie beim Erstellen dieser Netzwerkressource nur die IP-Adresse des Webkonferenzservers an (z. B. 10.10.50.60/32).
2. Erweitern Sie im linken Bereich die Benutzergruppe "Default".
3. Ziehen Sie die Netzwerkressource "Gastressource" aus dem rechten Bereich der Registerkarte **Access Policy Manager** auf **Network Policies** der Gruppe "Default" im linken Bereich.

Hinweis: Wenn sich Benutzer anmelden und keine Gruppeninformationen abrufen kann, werden immer die Einstellungen der Gruppe "Default" verwendet.

Mit diesen Schritten bewirkt der Administrator Folgendes:

- Silvio Branco und Lisa Marth können die Benutzeranmeldeinformationen "Gast\Silvio Branco" oder "Gast\Lisa Marth" zur Authentifizierung beim Bereich "Gast" auf dem Access Gateway eingeben. Bei der Authentifizierung müssen Silvio Branco und Lisa Marth den Bereichsnamen als Bestandteil ihrer Benutzeranmeldeinformationen einschließen, da sie sich bei einem Bereich authentifizieren, der nicht der Authentifizierungsbereich "Default" ist.

  Silvio Branco und Lisa Marth verwenden außerdem das Kennwort, das der Administrator für sie für die Authentifizierung beim Access Gateway festgelegt hat. Der Administrator hat diese Kennwörter beim Erstellen von Silvio Branco und Lisa Marth als lokale Benutzer auf dem Access Gateway eingegeben.

- Silvio Branco und Lisa Marth dürfen auf alle in der Zugriffssteuerungsliste der Benutzergruppe "Default" definierten Ressourcen zugreifen, da "No authorization" als Autorisierungstyp des Bereichs "Gast" angegeben ist.

  In diesem Beispiel können Silvio Branco und Lisa Marth nur auf den Webkonferenzserver im internen Netzwerk zugreifen, weil nur diese Netzwerkressource für die Benutzergruppe "Default" definiert ist.

Szenario für das Konfigurieren der lokalen Autorisierung für lokale Benutzer

Durch geringfügiges Ändern der unter "Szenario für das Erstellen von Gastkonten mit der Liste "Local Users"" beschriebenen Konfiguration kann der Administrator lokalen Benutzern (Lisa Marth und Silvio Branco) die gleichen Zugriffsrechte auf die internen Netzwerkressourcen gewähren wie den Benutzern aus den Bereichen Vertrieb oder Technik.

In diesem Szenario wird das Konzept der lokalen Autorisierung für lokale Benutzer erläutert.

Beispiel: Der Administrator möchte Lisa Marth und Silvio Branco die gleichen Zugriffsrechte gewähren wie den Benutzern aus dem Bereich "Technik". Zu diesem Zweck könnte der Administrator zwei Arbeitsschritte ausführen:

- Ändern des Autorisierungstyps des Bereichs Gast in lokale Autorisierung
- Zuweisen der lokalen Benutzer Lisa Marth und Silvio Branco zur Gruppe "Außendiensttechniker" auf dem Access Gateway

Um die lokalen Benutzer Lisa Marth und Silvio Branco der Gruppe "Außendiensttechniker" auf dem Access Gateway zuzuweisen, geht der Administrator wie folgt vor:

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Erweitern Sie den Eintrag **User Groups** und dann den Eintrag **Local Users**.
3. Klicken Sie unter **Local Users** auf den Namen Lisa Marth und ziehen Sie ihren Namen auf **Local Group Users** unter der Benutzergruppe "Außendiensttechniker".
4. Klicken Sie unter **Local Users** auf den Namen Silvio Branco und ziehen Sie seinen Namen auf **Local Group Users** unter der Benutzergruppe "Außendiensttechniker".

Nach Ausführung dieses Arbeitsschritts treffen die beiden folgenden Aussagen zu:

- Silvio Branco und Lisa Marth können die Benutzeranmeldeinformationen "Gast\Silvio Branco" oder "Gast\Lisa Marth" zur Authentifizierung beim Bereich "Gast" auf dem Access Gateway eingeben.
- Silvio Branco und Lisa Marth dürfen auf alle in der Zugriffssteuerungsliste der Benutzergruppe "Außendiensttechniker" definierten Ressourcen zugreifen, da "Local authorization" als Autorisierungstyp für den Bereich "Gast" angegeben ist.

  Hierdurch erhalten lokale Benutzer dieselbe Autorisierung wie die Benutzergruppe auf dem Access Gateway, der sie zugewiesen sind. Ihnen wird nicht die mit der Benutzergruppe "Default" auf dem Access Gateway verknüpfte Autorisierung erteilt, wie es der Fall ist, wenn "No authorization" für den Authentifizierungsbereich "Gast" aktiviert ist.

Problembehandlung beim Access Gateway

Im Folgenden wird erläutert, was Sie bei Problemen tun können, die beim Einrichten und Verwenden des Access Gateways auftreten.

Problembehandlung bei Webinterface-Verbindungen

In diesem Abschnitt werden Probleme erläutert, die beim Herstellen einer Verbindung zum Webinterface auftreten können.

Das Webinterface wird angezeigt, ohne dass Anmeldeinformationen eingegeben wurden

Wenn Sie die Webadresse für das Access Gateway eingegeben haben, wird das Webinterface angezeigt, ohne dass der Benutzername und das Kennwort eingegeben werden mussten. Die Ursache ist, dass Sie die Portalseitenauthentifizierung deaktiviert haben. Aktivieren Sie im Administration Tool auf der Registerkarte **Global Cluster Policies** unter **Advanced options** die Option **Enable logon page authentication**.

Wenn diese Option deaktiviert ist, wird nicht authentifizierter Netzwerkverkehr an das Webinterface gesendet. Dies ist zwar eine gültige Konfiguration, Sie müssen aber sicherstellen, dass das Webinterface in der DMZ ist.

Nach dem Anmelden werden keine Anwendungen angezeigt

Benutzern, die sich am Access Gateway anmelden, werden die Anwendungen nicht angezeigt. Das Message Center gibt an, dass keine Domäne festgelegt wurde.

Standardmäßig übergibt das Access Gateway nur den Benutzernamen und das Kennwort an das Webinterface. Um dieses Problem zu beheben, konfigurieren Sie in der Access Management Console eine Standarddomäne oder eine Domänenliste, an denen sich der Benutzer anmelden kann. Das Webinterface verwendet die in der Liste an erster Stelle stehende Domäne als Standarddomäne.

Benutzer, die sich am Access Gateway anmelden, sehen zwar das Webinterface, nicht aber ihre Anwendungen. Das Message Center gibt an, dass die Anmeldeinformationen des Benutzers ungültig sind.

Die wahrscheinlichste Ursache für diese Fehlermeldung ist, dass die Benutzer sich am Access Gateway mit Nicht-LDAP-Anmeldeinformationen von einer anderen Domäne als der Domäne anmelden, für die das Webinterface eingerichtet ist. Zur Lösung dieses Problems müssen Sie sicherstellen, dass die Standarddomäne auf dem Server, auf dem das Webinterface ausgeführt wird, mit dem Standardbereich im Access Gateway identisch ist. Stellen Sie außerdem sicher, dass das Access Gateway für LDAP-Authentifizierung konfiguriert ist und dass der LDAP-Server ein Domänencontroller in derselben Domäne wie das Webinterface ist.

Benutzer könnten sich auch mit einem Bereichsnamen am Access Gateway anmelden, aber der Bereichsname ist nicht derselbe wie der Domänenname. Bereichsnamen müssen mit den entsprechenden Active Directory-Domänennamen übereinstimmen. Damit sich Benutzer mit einem anderen Bereichsnamen als dem des Standardbereichs anmelden können, geben Sie den Bereichsnamen und den Benutzernamen ein, z. B. *Bereichsname\Benutzername*. Wenn sich die Benutzer am Access Gateway anmelden, werden dann der Bereichsname und der Benutzername an das Webinterface übergeben. Das Webinterface wandelt den Bereichsnamen und den Benutzernamen in den Domänennamen und Benutzernamen um.

Benutzer werden zu einer Anmeldeseite geleitet, auf der sie zum Starten des Access Gateway Plug-ins aufgefordert werden

In den Gruppeneigenschaften der Standardgruppe, bzw. der Gruppe mit der höchsten Priorität, des Benutzers ist auf der Registerkarte **Gateway Portal** die Option **Use the multiple logon option page** aktiviert. Wenn Sie Benutzern keinen Zugriff auf das Access Gateway Plug-in geben möchten, deaktivieren Sie dieses Kontrollkästchen. Weitere Informationen hierzu finden Sie unter "Konfigurieren einer Portalseite mit mehreren Anmeldeoptionen" auf Seite 178.

So deaktivieren Sie die Seite mit mehreren Anmeldeoptionen

1. Klicken Sie mit der rechten Maustaste auf der Registerkarte **Access Policy Manager** auf eine Gruppe und klicken Sie dann auf **Properties**.
2. Deaktivieren Sie auf der Registerkarte **Gateway Portal** die Option **Use the multiple logon option page** und klicken Sie auf **OK**.

Sonstige Probleme

In diesem Abschnitt werden bekannte Probleme, die im Zusammenhang mit dem Access Gateway auftreten, sowie entsprechende Lösungsvorschläge beschrieben.

Lizenzdatei stimmt nicht mit dem Access Gateway überein

Wenn Sie versuchen, eine Lizenzdatei auf dem Access Gateway zu installieren, wird die Fehlermeldung "License file does not match any Access Gateway's" angezeigt. Auf dem Access Gateway ist dann bereits eine Lizenzdatei installiert. Wenn Sie eine neue Lizenzdatei hochladen möchten, muss die alte Lizenz entfernt werden.

So installieren Sie eine neue Lizenzdatei auf dem Access Gateway

1. Wählen Sie auf der Registerkarte **Access Gateway Cluster** das Access Gateway aus, dem Sie die Lizenz hinzufügen möchten.
2. Klicken Sie auf der Registerkarte **Licensing** neben **Remove all license files** auf **Remove All**.
3. Starten Sie das Access Gateway neu.

4. Klicken Sie auf der Registerkarte **Licensing** neben **Install a license file** auf **Browse** und navigieren Sie zur Lizenzdatei.
5. Klicken Sie auf **Öffnen**, um die Datei zu installieren.
6. Starten Sie das Access Gateway neu.

Definieren von Subnetzeinschränkungen für zugängliche Netzwerke

Im Feld **Accessible networks** auf der Registerkarte **Global Cluster Policies** können bis zu 24 Subnetze definiert werden. Wenn mehr als 24 Subnetze angegeben werden, ignoriert das Access Gateway die überzähligen Einträge.

Virtualisierungssoftware

Wenn Benutzer sich am Access Gateway von zwei Computern anmelden, auf denen Virtualisierungssoftware ausgeführt wird, wie z. B. Xen, VMWare, oder Hyper-V, und die Virtualisierungssoftware die gleiche MAC-Adresse für beide Computer verwendet, lässt Access Gateway nicht zu, dass beide Instanzen der Clientsoftware gleichzeitig ausgeführt werden. Das Access Gateway verwendet die MAC- Adresse zum Verwalten der Lizenzen und lässt immer nur eine Benutzersitzung pro MAC-Adresse gleichzeitig zu.

ICMP-Übertragungen

Wenn eine ICMP-Übertragung aus irgendeinem Grund fehlschlägt, gibt das Access Gateway eine "Request timed out"-Fehlermeldung zurück. Wenn ein Benutzer versucht, das Access Gateway zu pingen, sendet es immer ein ICMP-Standardpaket an den Remotezielhost. Sämtliche Optionen, wie z. B. das Erhöhen der Größe der ICMP-Nutzlast, werden vom Access Gateway nicht anerkannt und auch nicht an den Remotehost gesendet.

Ping-Befehl

Das Access Gateway sendet grundsätzlich denselben ping-Befehl aus, und dies unabhängig von den Optionen, die beim Pingen von einem Clientgerät aus angegeben werden.

LDAP-Authentifizierung

Wenn das Access Gateway für die Verwendung der LDAP-Authentifizierung und -Autorisierung konfiguriert ist, werden die LDAP-Gruppeninformationen nicht zum automatischen Ausfüllen des Gruppenfelds im Administration Tool verwendet.

Endpoint Policies (Endpunktrichtlinien)

Bei der Auswertung der Kombination von Endpunktrichtlinien einer Gruppe berücksichtigt das Access Gateway nicht die Gruppenprioritäten, sodass miteinander in Konflikt stehende Richtlinien u. U. nicht korrekt aufgelöst werden. Nur die Richtlinie, die im Ausdruck zuletzt aufgeführt wird, gilt. Wenn z. B. für eine Gruppe die Richtlinie "ProzessA" und für eine andere Gruppe die Richtlinie "!ProzessA" gilt und die Kombination aus diesen beiden Richtlinien "ProzessA und !ProzessA" ist, gilt nur die Richtlinie "!ProzessA".

Netwerkressourcen

Bei hinzugefügten Netzwerkressourcen erkennt das Access Gateway nicht die CIDR-Notation der Adresse *IP-Adresse*/0. Wenn Sie z. B. eine Ressourcengruppe hinzufügen möchten, die den Zugriff auf alle Ressourcen erlaubt, geben Sie für die Adresse "0.0.0.0/0.0.0.0" statt "0.0.0.0/0" an.

Internes Failover

Wenn das interne Failover aktiviert ist und der Administrator eine Verbindung zum Access Gateway hergestellt hat, ist das Administration Tool über diese Verbindung nicht erreichbar. Aktivieren Sie zum Beseitigen dieses Problems das IP-Pooling und stellen Sie dann eine Verbindung zur niedrigsten IP-Adresse im IP-Pool auf Port 9001 her. Wenn der IP-Pool z. B. bei 10.10.3.50 beginnt, stellen Sie die Verbindung zum Administration Tool unter Verwendung von 10.10.3.50:9001 her. Informationen zum Konfigurieren von IP-Pools finden Sie unter "Aktivieren von IP-Pooling" auf Seite 159.

Zertifikatsignierung

Zahlreiche Citrix Serverkomponenten unterstützen SSL/TLS, z. B. Access Gateway, Secure Gateway und SSL Relay. Alle diese Komponenten unterstützen Serverzertifikate, die von einer öffentlichen oder einer privaten Zertifizierungsstelle (CA, Certificate Authority) ausgegeben wurden. Beispiele für öffentliche Zertifizierungsstellen sind Organisationen wie Verisign und Thawte. Private Zertifizierungsstellen werden durch Produkte, wie z. B. Microsoft Zertifikatdienste, implementiert.

Zertifikate, die von einer privaten Zertifizierungsstelle signiert wurden, werden mitunter als *Unternehmenszertifikate* oder *selbst signierte Zertifikate* bezeichnet. Der Begriff "selbst signiertes Zertifikat" ist in diesem Zusammenhang technisch unkorrekt, da die Zertifikate von der privaten Zertifizierungsstelle signiert werden. Wirklich selbst signierte Zertifikate werden hingegen nicht von einer Zertifizierungsstelle signiert und auch nicht von Citrix Serverkomponenten unterstützt, da dann keine vertrauenswürdige Zertifizierungsstelle dahinter steht. Wie bereits oben erwähnt, werden aber von einer privaten Zertifizierungsstelle ausgegebene Zertifikate von Citrix Serverkomponenten unterstützt, da der privaten Zertifizierungsstelle vertraut werden kann.

Zertifikatsperrlisten

Zertifikatsperrlisten (Certificate Revocation Lists, CRLs) können nicht vom Administrator konfiguriert werden. Wenn ein Benutzer eine Verbindung zum Access Gateway unter Verwendung eines Clientzertifikats herstellt, verwendet das Access Gateway die CRLDistributionPoints-Erweiterung im Clientzertifikat, sofern vorhanden, um über HTTP nach relevanten CRLs zu suchen. Das Clientzertifikat wird dann mit diesen CRLs abgeglichen.

Netzwerkmeldungen an nicht vorhandene IP-Adressen

Wenn die auf das Access Gateway hochgeladene Datei sdconf.rec ungültig ist, sendet das Access Gateway u. U. Meldungen an nicht vorhandene IP-Adressen. Netzwerküberwachungseinrichtungen könnten dies als Netzwerkspamming einstufen.

Dieses Problem können Sie beseitigen, indem Sie eine gültige sdconf.rec-Datei auf das Access Gateway hochladen.

Das Access Gateway startet nicht und die serielle Konsole ist leer

Überprüfen Sie die folgenden Elemente auf ihre korrekte Einrichtung:

- Die serielle Konsole verwendet den richtigen Port und der physische Port stimmt mit dem logischen Port überein.
- Das Kabel ist ein Nullmodemkabel.
- Die COM-Einstellungen der seriellen Kommunikationssoftware sind wie folgt festgelegt: 9600Bit/s, 8 Datenbits, keine Parität und 1 Stoppbit.

Zugriff auf das Administration Tool nicht möglich

Wenn das Access Gateway offline ist, ist das Administration Tool nicht verfügbar. Zum Ausführen von Aufgaben wie dem Anzeigen des Systemprotokolls und dem Neustarten des Access Gateways können Sie das Administration Portal verwenden.

Kommunikation zwischen Geräten und dem Access Gateway nicht möglich

Überprüfen Sie die folgenden Elemente auf ihre korrekte Einrichtung:

- Der auf der Registerkarte **General Networking** im Access Gateway Administration Tool angegebene vollqualifizierte Domänenname ist außerhalb Ihrer Firewall verfügbar.
- Sämtliche Änderungen, die in der seriellen Konsole des Access Gateways oder im Administration Tool vorgenommen wurden, wurden gesendet.

Verwenden von Strg+Alt+Entf zum Neustarten des Access Gateways nicht möglich

Die Neustartfunktion auf dem Access Gateway ist deaktiviert. Sie müssen das Gerät mit dem Administration Tool neu starten und herunterfahren.

Sitzungen mit SSL Version 2 und Zertifikatketten auf mehreren Ebenen

Wenn Zwischenzertifikate (Zertifikate mit mehreren Ebenen) Teil Ihres sicheren Zertifikatsuploads sind, stellen Sie sicher, dass die Zwischenzertifikate in der hochzuladenden Zertifikatdatei enthalten sind. SSL Version 2 unterstützt die Zertifikatsverkettung nicht. Alle Zertifikate, die mehr als eine Ebene besitzen, müssen sämtliche Zwischenzertifikate enthalten, da das System anderenfalls unbrauchbar werden könnte. Informationen dazu, wie Sie der hochzuladenden Zertifikatdatei Zwischenzertifikate hinzufügen können, finden Sie unter "Sichern von Verbindungen mit digitalen Zertifikaten" auf Seite 223.

H.323-Protokoll

Das Access Gateway unterstützt das H.323-Protokoll nicht. Anwendungen, die das H.323-Protokoll verwenden, wie z. B. NetMeeting von Microsoft, können mit dem Access Gateway nicht verwendet werden.

Zertifikate mit 512-Bit-Schlüsselpaaren

Verwenden Sie zum Konfigurieren von Zertifikaten keine 512-Bit-Schlüsselpaare, da diese oft Opfer von Brute-Force-Angriffen werden.

Laufwerkszuordnung kann nicht mit einer Anwendungsrichtlinie eingeschränkt werden

Sie können nicht mit einer Anwendungsrichtlinie Benutzeraktivitäten, die direkt innerhalb des Windows-Betriebssystems verarbeitet werden, z. B. die Laufwerkszuordnung, einschränken. Hierfür müssen Sie eine Netzwerkgruppenrichtlinie verwenden.

Beispiel: Wenn Sie verhindern möchten, dass Benutzer in der Standardbenutzergruppe in Windows-Explorer eine Verknüpfung mit Laufwerken im Subnetz 10.51.251.0/24 herstellen, müssen Sie eine Gruppenressource erstellen, in der dieses Subnetz angegeben wird, und diese Ressource der Standardgruppe zuweisen. Verweigern Sie dann den Zugriff auf diese Netzwerkressource.

Sie können den Zugriff nicht durch Erstellen einer Anwendungsrichtlinie für Windows-Explorer einschränken, in die eine Netzwerkressource eingebettet ist, auf die der Zugriff Netzwerkressource verweigert ist.

Citrix Access Gateway Plug-in

Es folgen Probleme mit dem Citrix Access Gateway Plug-in.

Access Gateway Plug-in-Verbindungen mit Windows XP

Wenn ein Windows XP-Benutzer eine Verbindung zum Access Gateway herstellt, den Computer abmeldet, ohne vorher die Verbindung mit dem Access Gateway Plug-in zu trennen, und sich dann wieder anmeldet, ist die Internetverbindung unterbrochen. Zum Wiederherstellen der Internetverbindung müssen Sie den Computer neu starten.

DNS-Namensauflösung mit Namensdienstanbietern

Wenn Benutzer ohne administrative Berechtigungen über Windows 2000 Professional oder Windows XP eine Verbindung zum Access Gateway herstellen, kann die DNS-Namensauflösung scheitern, wenn der Client einen Namensdienstanbieter verwendet. Dieses Problem lässt sich beheben, indem die Verbindung nicht mit dem DNS-Namen, sondern mit der IP-Adresse des Computers hergestellt wird.

Funktion zum automatischen Aktualisieren

Die Access Gateway Plug-in-Funktion zum automatischen Aktualisieren funktioniert nicht, wenn der Client für das Herstellen der Verbindung über einen Proxyserver konfiguriert ist.

Von Windows Server 2003-Computern ausgehende Clientverbindungen

Wenn von einem Windows Server 2003-Computer aus eine Verbindung zum Access Gateway hergestellt wird, der sein eigener DNS-Server ist, funktionieren die lokale und die öffentliche DNS-Auflösung nicht. Dieses Problem können Sie beheben, indem die Windows Server 2003-Netzwerkeinstellungen auf einen anderen DNS-Server verweisen.

NTLM-Authentifizierung

Das Access Gateway Plug-in unterstützt nicht die NTLM-Authentifizierung bei Proxyservern. Bei Proxyservern wird lediglich die einfache Authentifizierung unterstützt.

WINS-Einträge

Wenn das Access Gateway Plug-in getrennt wird, werden WINS-Einträge nicht von dem Computer entfernt, auf dem das Plug-in ausgeführt wird.

Benutzer von Einwählverbindungen erhalten keine WINS-Serverzuordnungen. Legen Sie zur Behebung dieses Problems die interne WINS-Adresse manuell fest oder verwenden Sie einen DNS-Server von Microsoft zum Festlegen der Domäne für die WINS-Suche.

Verwendung von Drittanbieter-Clientsoftware

Wenn auf dem Computer eines Benutzers das Access Gateway Plug-in ausgeführt wird, auf diesem Computer aber auch VPN-Software eines Drittanbieters installiert ist und die Verbindungen nicht korrekt über das Access Gateway ausgeführt werden, vergewissern Sie sich, dass die Drittanbieteranwendung deaktiviert oder ausgeschaltet ist. Testen Sie anschließend die Access Gateway Plug-in-Verbindung noch einmal.

Index

A

Access Gateway
- Administration Tools 181
- Betriebsmodi 16
- Herunterfahren 195
- Initialisieren 195
- Lizenzierung für mehrere Geräte 48
- Neustart 42, 194
- Software neu installieren 189
- Statistik 221
- Überwachung 221
- Upgrades 186
- Verbindungen 16
- Wartung 181

Access Gateway Advanced Edition 17, 30
- Clientzertifikate 167
- inaktive Server 31

Access Gateway Plug-in 16
- Anmelden 152, 178
- automatische Aktualisierung 277
- Firewalls verwenden 141
- Installation 152
- Installation mit Gruppenrichtlinie 146
- IP-Pooling 159
- Konfigurieren eines Proxyservers 144
- Linux-Unterstützung 156
- MSI-Installation 145
- MSI-Paket 19
- Proxies verwenden 141
- Proxyserver einrichten 154
- Split-DNS 161
- Status 197
- Systemanforderungen 138
- Upgrade erzwingen 150
- Upgrade verhindern 150
- Upgradeaufforderung 150
- Upgrades von früheren Versionen 149
- Verbinden mit früheren Versionen 149
- Verbindungsprotokolle 217
- Verwenden mit Proxyservern 144
- VPN-Software von Drittanbietern 278
- Windows 2003 Server 277
- Windows XP 277
- Zugriffssteuerungsliste 156

Access Gateway Plug-in für Linux 19, 156

ACL siehe Zugriffssteuerungsliste

Administration Desktop 18–19, 215

Administration Portal 184
- Administration Tool 181
- Administratorkennwort 184
- externen Zugriff deaktivieren mit Administration Tool 186
- externen Zugriff mit der seriellen Konsole deaktivieren 36
- Port 23
- Protokollierung 185
- verfügbare Downloads 184
- Wartung 185
- Zertifikate, Installation 54

Administration Tool
- Downloads 184
- Installation 38, 182
- internes Failover 273
- Kein Zugriff 275
- mehrere Versionen 183
- Port 23
- Protokollierung 185
- Rückwärtkompatiblität 19

Administratorkennwort 184
- Administration Portal 184
- serielle Konsole 36

Aktualisieren von Lizenzen 49

Anmeldeseite 118
- Authentifizierung aktivieren 172
- Authentifizierung deaktivieren 177

Anmeldeskripte 162

Anwendungsrichtlinien 118, 126
Konfigurationsbeispiel 258
Laufwerkszuordnung kann nicht eingeschränkt werden 276
Zulassen und Verweigern 125
Archiv des Systemprotokolls 216
Asymmetrische Verschlüsselung 226
Authentifizierung 92
Aktivieren von RSA SecurID 97
Anmeldeseite aktivieren 172
Anmeldeseite deaktivieren 177
Benutzergruppen 115
Bereiche 76
erweiterte Optionen 106
Gemalto Protiva 18, 102
keine Autorisierung 74
Konfigurieren 72
LDAP 81, 139
LDAP-Konfigurationsbeispiel 244, 252
lokal 78, 139
Lokale Benutzer 79
Netzwerkunterbrechung 158
NTLM 104, 139, 277
RADIUS 90, 139
RSA SecurID 95, 139
SafeWord 99, 139
Standardbereich 75
Zertifikate 227
Zweimethodenauthentifizierung 108
Authentifizierungstypen 26
Autorisierung 74
LDAP 81, 86
LDAP-Konfigurationsbeispiel 244
Lokale Benutzer 79
NTLM 105
RADIUS 90, 93
SafeWord 101

B

Benutzer
mehreren Gruppen hinzufügen 121
Netzwerkresourcen 122
Netzwerkzugriff 112
Benutzergruppen
Authentifizierung 115
Benutzer 115
Eigenschaften 119, 159
Entfernen 119
Erstellen 118
IP-Pooling 159
Konfigurieren 115
lokal 116
mehrere 118
Portalseite 177
Ressourcen 120
Ressourcenzugriffssteuerung 125
Sitzungstimeout aktivieren 163
Split-DNS 161
Überblick 115
Benutzergruppeninformationen 115
Benutzernamensvariable für Portalseite 175
Benutzersitzungstimeout 163
Benutzerverbindungen
Access Gateway Plug-in 137
Bereiche
Entfernen 78
Erstellen 76
Bereichsbasierte Authentifizierung
Standardbereich 75
Bereitstellung
Access Gateway Advanced Edition 30
Authentifizierungsunterstützung 26
Citrix XenApp 27
Citrix XenDesktop 27
Cluster 203
Double-Hop-DMZ 27
einzelne DMZ 22
Failover 28, 212
gesichertes Netzwerk 24
Load Balancer 28, 206
Mehrere Access Gateway-Geräte 201
Sicherheitsüberlegungen 25
Webinterface 27
Bereitstellungsoptionen 22
Betriebsmodi 16
Branch Repeater 136

C

CAs Siehe Zertifizierungsstellen (Certificate Authorities)
Citrix Branch Repeater 136
Repeater Plug-in 136
Citrix Education 13
Citrix Preferred Support Services 12
Citrix Presentation Server Clients siehe Citrix XenApp Plug-ins
Citrix Repeater Plug-in 136
Citrix Solutions Advisers 12

Citrix XenApp 16, 118
Bereitstellung 27
Split-Tunneling 115
Citrix XenApp Plug-ins 16
Citrix XenDesktop 18
Bereitstellung 27
Clients, Stammzertifikate 167
Clientverbindungsprotokolle 217
Clientzertifikate 165
Access Gateway Advanced Edition 167
Kriterien festlegen 165
Clientzugriff
IP-Pooling 118
Portalseite 177
Ressourcenzugriffssteuerung 125
Sitzungstimeout 117
Split-DNS 118
Cluster
Erstellen 203
RSA SecurID 98
Computer
Ruhezustand 158
Standby-Modus 158
CRLs (Certificate Revocation Lists) siehe Zertifikatsperrlisten

D

Datum einstellen 66
Desktopfreigabe 19
DNS
Access Gateway Plug-in-Fenster 156
Failover auf lokales 58
Namensauflösung 277
Servereinstellungen 58
DNS/WINS siehe Name Service Providers
Dokumentation, Download 184
Dokumentation, Produkt 12
Domänenanmeldeskripte 162
Double-Hop-DMZ 27
TCP/IP-Einstellungen 41
Downloads
Access Gateway-Dokumentation 184
Administration Portal 184
Administration Tool 184
Portalseitenvorlagen 184
Duplex Mode 39
Dynamisches Routing 60–61
RIP-Authentifizierung aktivieren 61
Dynamisches Routing, Speichern in statischer Routingtabelle 62

E

Eigenschaften
Access Gateway Plug-in 197
Benutzergruppen 119
Gruppen 117
Eigenständige Bereitstellung 16
Eingabeaufforderung
Erstellen mehrerer Stammzertifikate 57
Endpunktressource
Entfernen 130
Konfigurieren 129
Endpunktrichtlinie 130
Ausdruck erstellen 132
Erstellen 131
gültige Operatoren 131
Problembehandlung 273
Entfernen Bereiche 78
Erweiterte Optionen
Authentifizierung 106
Ethereal Network Analyzer, Unverschlüsselter Datenverkehr 142
Express Setup, Serielle Konsole 36

F

Failover 28
Bereitstellung 212
DNS-Server 58
internes 161
Konfigurieren 212
Firewall
Access Gateway Plug-in 141
Lizenzierung 49
McAfee Personal Firewall Plus 198
Norton Personal Firewall 198
Sygate Personal Firewall 198
Tiny Personal Firewall 199
ZoneAlarm Pro 199
FTP, Konfigurieren für Clients 143

G

Gemalto Protiva 18, 102
Gemalto Protiva-Authentifizierung 26
Gemeinsamer geheimer Schlüssel 98
Geschwindigkeitsmodus 39
Gruppenattribute, LDAP-Autorisierung 87
Gruppeneigenschaften 117
Gruppenpriorität 118, 134
Gruppenressourcen 118

Gruppenrichtlinie, Installation des Access Gateway Plug-ins 146
Gruppen, Benutzer hinzufügen 121
Gruppenzugriff, Konfigurationsbeispiele 254

H

Hardwareinstallation 35
Herunterfahren des Access Gateways 195
Hostscanregeln siehe Endpunktressource
HOSTS-Datei bearbeiten 59
HyperTerminal 37, 54
H.323-Protokoll 276

I

IAS siehe Internet Authentication Server
ICMP siehe Internet Control Message Protocol
ICMP-Übertragungen 272
IEEE 802.11-Unterstützung 33
IETF, siehe Internet Engineering Taskforce
Inaktive Server, Access Gateway Advanced Edition 31
Inaktive Sitzung, Timeout 163
Inaktivitätstimeout 117
Initialisieren des Access Gateways 195
Installation 38
  Access Gateway 33
  Access Gateway Plug-in 152
  Access Gateway Plug-in für Linux 156
  Access Gateway Plug-in mit MSI-Paket 145
  Administration Tool 38, 182
  einzelne DMZ 23
  Hardware 35
  Kreuzkabel 38
  Lizenzen 47
  Material 34
  mehrere Stammzertifikate 57
  Netzwerkkabel 38
  Portalseite 176
  Stammzertifikate 56
  Zertifikate 51, 53–54
  Zertifikate, Administration Portal 54
Internes Failover 161
  Administration Tool 273
Internet Authentication Server, RADIUS 90
Internet Control Message Protocol
Internet Engineering Taskforce 224
Internet-Sicherheitsprotokolle 224
IP-Pooling 118, 159
ISO X.509-Protokoll 227

K

Kennwort, Administrator 184
Kennwortbeschriftung 155
Kennwörter
  Administrator 36, 184
  privater Schlüssel für Zertifikat 52
Kennwortfelder 155
Kennwortfelderbeschriftung 110
Kioskmodus 19
Knowledge Center 12
Knowledge Center-Benachrichtigungen 13
Konfiguration
  Anwendungsrichtlinie 126
  Authentifizierung ohne Autorisierung 74
  Benutzergruppen 115, 118
  Endpunktressource 129
  Endpunktrichtlinie 130
  Lokale Benutzer 79
  Netzwerkressource 123
  Ressourcengruppen 117
  Split-Tunneling 115
  Standardgateway 40
  Vorauthentifizierungsrichtlinien 135
Konfigurationsbeispiele
  Anwendungsrichtlinien 258
  Gruppenzugriff bereitstellen 254
  LDAP-Authentifizierungsbereich 252
  lokale Autorisierung 266
  lokale Benutzer 262
  Netzwerkzugriff 243
  zugängliche Netzwerke 251
Konfigurieren für Gruppen 130
Kreuzkabel 34, 38
Kryptografie 225
  asymmetrische Verschlüsselung 226
  geheimer Schlüssel 225
  öffentlicher Schlüssel 225
  symmetrischer Schlüssel 225
Kryptographie, Konzepte 224
Kulanzzeitraum, Lizenzen 50

L

Laufwerkszuordnung, Zugriff einschränken 276
LDAP-Authentifizierung 26, 81, 139
  Gruppenmitgliedschaften 86
  Konfigurationsbeispiele 244, 252
  Konfigurieren 83
  Ports 81
  Verzeichnisattribute 89
  Zertifikate 89
LDAP-Autorisierung 81, 86
  Gruppenattribute 87
  Konfigurationsbeispiele 244
  Konfigurieren 87
LDAP-Browser 89
Linkmodus, serielle Konsole 36
Linux-Unterstützung (Client) 156
  Befehlszeilenoptionen 157
  Client entfernen 157
  Neustart 157
  Status prüfen 157
Lizenzen
  Abrufen 46
  File does not match (Fehlermeldung) 271
  Informationen aktualisieren 49
  Installation 43, 47
  Kulanzzeitraum 50
  mehrere Geräte 48
  Ports 49
  Statistik 45
  Testen 50
  Update 49
Lizenzierung
  Firewallregeln 49
  XenDesktop 19
Lizenzprotokolle 49
Lizenzserver 43, 48
Lizenztypen 44
Load Balancer
  Einstellen als Standardgateway 210
  Geräte bereitstellen mit 206
  Installations- und Konfigurationsprobleme 207
Load Balancing 28
Lokale Authentifizierung 78, 139
Lokale Autorisierung
  Konfigurationsbeispiele 266
Lokale Benutzer 115
  Konfigurationsbeispiel 262
  Konfigurieren 79
  mehrere Benutzergruppen 118
Lokale Benutzergruppen 116

M

Material, Access Gateway Installation 34
Maximum Transmission Unit 40
McAfee Personal Firewall Plus 198
Mehrere Anmeldeoptionen
  Portalseite 178
MSI-Installation, Access Gateway Plug-in 19, 145
MTU siehe Maximum Transmission Unit
Multi Router Traffic Grapher 219

N

Name Service Providers 58, 278
  Namensauflösung, Problembehandlung 277
NetMeeting 276
Network Time Protocol 66
Netzwerk
  Flooding 274
  Routetracing 222
  Spamming 274
  Split-Tunneling 114
  Verbindungsfehler 275
Netzwerkadapter, TCP/IP-Einstellungen konfigurieren 39
Netzwerkaktivitätstimeout 117
Netzwerkgeschwindigkeit, Einstellung 39
Netzwerkinaktivitätstimeout 163
Netzwerkkabel 34
  Installation 38
  TCP/IP konfigurieren 38
Netzwerkressourcen 16, 118
  CIDR nicht erkannt 273
  Erstellen 123
  Gruppen hinzufügen 124
  Konfigurieren 122
  Zulassen und Verweigern 125
Netzwerkrouting 112
Netzwerküberwachung
  Packet Capture 222
  Portscan 222
Netzwerkunterbrechung, Authentifizierung 158
Netzwerkzugriff
  Benutzern bereitstellen 112
  Konfigurationsbeispiele 243
  Konfigurieren 69
  Routing 112
Neue Produktnamen 14
Neustart des Access Gateways 42, 194
Neustarten des Access Gateways 275
Node Secret 98
Norton Personal Firewall 198

NTLM-Authentifizierung 26, 104, 139, 277
NTLM-Autorisierung 105
NTP siehe Network Time Protocol

O

Öffentliche Zertifizierungsstellen 232
Optimierung, Citrix Branch Repeater 136

P

Packet Capture 222
Packliste 34
Ping
    Serielle Konsole 36
    Befehl 36, 272
PKI, siehe Public Key Infrastructure
Portalseite 118
    Anpassen 175
    Benutzernamensvariable 175
    Downloadvorlagen 174
    Installation 176
    Konfigurieren 177
    mehrere Anmeldeoptionen 178
    Standard 67
    Verbinden mit 67
    Vorlagen 174
    Vorlagen herunterladen 184
Ports
    Administration Portal 23
    Administration Tool 23
    einzelne DMZ 23
    LDAP-Verbindungen 81
    Lizenzierung 49
    Umleitung 41
Portscan 222
Portumleitung 41
Presentation Server Clients siehe Citrix XenApp Plug-ins
Private Zertifizierungsstellen 232
Privater Schlüssel
    Entschlüsseln 235
    Installation über Windows-Computer 55
    kennwortgeschützt 52
    Kombinieren mit signiertem Zertifikat 237
Problembehandlung
    Webinterface 269
Produktdokumentation 12
Protokollierung
    Administration Portal 185
    Administration Tool 185
    Clientverbindungsprotokolle 217
    Serielle Konsole 36
Proxyserver
    Konfigurieren 144
    Konfigurieren für Access Gateway Plug-in 144, 154
Public Key Encryption 227
Public Key Infrastructure 224

R

RADIUS-Authentifizierung 26, 90, 139
    Konfigurieren 92
    Konfigurieren Internet Authentication Server 90
    SafeWord 100
RADIUS-Autorisierung 90
    Konfigurieren 93
Real-Time Monitor 19
Ressourcen
    Konfigurieren für Benutzergruppen 125
Ressourcengruppen 122
    Entfernen von Benutzergruppen 126
    Konfigurieren 117
Richtlinien
    Anmeldeseiten 172
    IP-Pooling 159
RIP-Authentifizierung 61
Routen
    dynamisches Routing konfigurieren 60–61
    statisch 62
    statisches Routing konfigurieren 62, 63
Routing
    Netzwerkzugriff 112
RSA ACE/Server
    Upload der sdconf.rec-Datei 97
    Zurücksetzen des Node Secrets 98
RSA SecurID-Authentifizierung 26, 95, 139
    Cluster 98
    IP-Adresse einrichten 97
    Konfigurieren 97

S

SafeWord-Authentifizierung 26, 99, 139
    Konfiguration 100
    unterstützte Produkte 99
SafeWord-Autorisierung 101
Schulung 13
sdconf.rec, ungültige Datei 274

sdconf.rec-Datei
Cluster 98
Ersetzen 97
Upload 97
Secure Socket Layer 140, 224
Verschlüsselungsart auswählen 169
Secure Ticket Authority 27
Serielle Konsole
Administration Portal aktivieren oder deaktiveren 36
Administratorkennwort 36
Optionen 36
Problembehandlung 275
TCP/IP-Einstellungen konfigurieren 36–37
Serielles Kabel 34
Serverzertifikat 228
Installation 233
Service 12
Sicherheit 25
Zertifikatverwaltung 25
Sicherheitskonzepte 223
Single Sign-on, Windows 148
Sitzungstimeout 117, 163
SNMP 219
Einstellungen 219
MIB-Gruppen 219
Protokolle aktivieren und anzeigen 219
Software neu installieren 189
Speichern, Systemkonfiguration 193
Split-DNS 118, 161
Split-Tunneling 114
Citrix XenApp 115
Konfigurieren 115
SSL siehe Secure Socket Layer
Stammzertifikate 167, 228
Erstellen über Befehlszeile 57
Installation 56, 168
Installation mehrerer 57
Standardbereich 75
Standardgateway konfigurieren 40
Standardlizenz 44
Standardportalseite 67
Standardzertifikat zurücksetzen 54
Statisches Routing 62
Beispiel 64
Entfernen 64
Hinzufügen 63
Testen 63
Statistik 221
Lizenzierung 45
Status, Access Gateway Plug-in 197
Subscription Advantage 13
Support 12–13
Sygate Personal Firewall 198
Syslog-Server, Systemprotokoll weiterleiten an 218
Systemanforderungen
Access Gateway Plug-in 138
USB-Speicher 191
Systemkonfiguration
Speichern 193
Wiederherstellen 193
Systemprotokoll
Anzeige 216
Archiv 216
Download 216
Filtern 216
Weiterleiten an Syslog-Server 218
Systemstatistik 221

T

TCP-Optionen erhalten
Citrix Branch Repeater 136
TCP/IP-Einstellungen
Double-Hop-DMZ 41
Konfigurieren in der seriellen Konsole 37
Konfigurieren mit Netzwerkkabel 38
Serielle Konsole 36
Technischer Support 12
Terminologieänderungen 14
Testzertifikate 233
Timeout
Benutzersitzung 117, 163
inaktive Sitzung 117, 163
Netzwerkinaktivität 117, 163
Websitzung 164
Tiny Personal Firewall 199
TLS siehe Transport Layer Security
Traceroute-Tool 222
Training 13
Transport Layer Security 140
TransPorts Layer Security 224

U

Überprüfungsintervall
Access Gateway Advanced Edition 31
Überwachungstools 221
Umleitung, Ports 41
Ungesicherte Verbindungen umleiten 41
Universelle Lizenz 44

Upgrades 13, 18
Access Gateway Plug-in 149
Access Gateway-Software 186
USB-Speicher, Systemanforderungen für Installation 191

V

Verbindungen
Access Gateway Advanced Edition 17
einzelne DMZ 23
Hardware 35
keine Clientverbindung 275
LDAP-Zertifikate 89
nur Access Gateway 16
simultan 16
Webadresse verwenden 150
Webinterface 16
Verbindungsprotokolle, Access Gateway Plug-in 217
Verschlüsselung
asymmetrisch 226
öffentlicher Schlüssel 227
Verschlüsselungssammlungen auswählen 169
Verschlüsselungssammlungen
Beschreibung 225
Verzeichnisattribute
LDAP 89
VMWare 272
Vorauthentifizierungsrichtlinien
Anmelden 179
Konfigurieren 135
Vorlagen
Administration Portal 184
Download über Portalseite 174
Portalseite 174, 184
Portalseite anpassen 175

W

Wartung
Administration Portal 185
Administration Tool 182
Webinterface 16, 118
Anmelden 178
Anwendungen nicht verfügbar 270
Bereitstellung 27
Problembehandlung 269
Zugriff ohne Anmeldeinformationen 269
Websitzungstimeout 164
Wiederherstellen der Systemkonfiguration 193
Windows
Anmeldeskripte 162
Single Sign-on 148
Windows NT LAN Manager siehe NTLM-Authentifizierung
Windows XP
Access Gateway Plug-in 277
WINS
Problembehandlung 278
WINS-Server
Access Gateway Plug-in-Fenster 156
Einstellung 58

X

XenDesktop 18
Lizenzen 19
XenDesktop-Verbindungslizenz 44
X.509-Standard 229

Z

Zeit
Einstellung 66
Synchronisieren
Zertifikate 25, 224, 227
512-Bit-Schlüsselpaare 276
Ablaufen 231
Access Gateway Advanced Edition 167
Authentifizierung 227
Client 165
Einstellung 53
Erneuerung 231
Erstellen mehrerer Stammzertifikate über Befehlszeile 57
Generieren für mehrere Ebenen 238
Hierarchie 229
Inhalt 228
Installation 51, 233
Installation mit Administration Portal 54
Installation mit Administration Tool 54
Installation über Windows-Computer 55
Kennwort für privaten Schlüssel 52
Ketten 229
Kombinieren mit privatem Schlüssel 237
LDAP-Verbindungen 89
Mehrere Ebenen und SSL Version 2 276
mehrere Stammzertifkate 57
Privat 232
privaten Schlüssel entschlüsseln 235
Probezeit 233
Serielle Konsole, Standard zurücksetzen 36

Server 228
Signieren 274
Sperrlisten 230
Stamm 167, 228
Stammzertifikat 56
Stammzertifikate unter Windows installieren 168
Test 233
Überprüfungsvorgang 232
Umwandeln in PEM-Format 235
untergeordnete 230
Zertifikatketten 229
Zertifikatsignieranforderung 52
Zurücksetzen auf Standardzertifikat 54
Zwischenzertifikat 230
Zertifikatketten 229
Zertifikatsignieranforderung, Überblick 52
Zertifikatsperrlisten 230, 274
Zertifizierungsstelle, Stammzertifikate abrufen 168
Zertifizierungsstellen 228
öffentlich 232
privat 232
untergeordnete 229
ZoneAlarm Pro 199
Zugängliche Netzwerke 114
Einschränkungen 272
Konfigurationsbeispiele 251
Zugängliche Netzwerke für Access Gateway, Access Gateway Plug-in-Fenster 156
Zugriff ohne Zugriffssteuerungsliste verweigern 113, 116
Zugriffssteuerungsliste 120
Access Gateway Plug-in-Eigenschaften 156
Zugriff ohne verweigern 113
Zugriff verweigern 116
Zulassen und Verweigern 125
Zweimethodenauthentifizierung 108